

MIGRACIÓN Y PUESTA EN MARCHA DE SERVICIOS A TRAVÉS DE ZENTYAL SERVER

Henry Andrés Fraile Gonzalez
e-mail: hafraileg@unadvirtual.edu.co
Andrés Londoño Pérez
e-mail: alondonoper@unadvirtual.edu.co
Edward Vicente Rincon Cortés
e-mail: evrinconc@unadvirtual.edu.co
Maryuri Andrea Ramirez Bedoya
e-mail: maramirezbed@unadvirtual.edu.co
Jose Alfredo Rodríguez Buitrago
e-mail: jarodriguezbui@unadvirtual.edu.co

RESUMEN: En este artículo se va a exponer de manera detallada la puesta en marcha de un servidor con sistema Zentyal 6.2, documentando el proceso de descarga e instalación. Adicional, se ahonda en el detalle paso a paso de cómo se configuran servicios en busca de satisfacer la necesidad en infraestructuras de IT.

PALABRAS CLAVE: Servidor, cliente, servicios, Zentyal, DHCP, DNS, Cortafuegos, Proxy, VPN.

1 INTRODUCCIÓN

Después de haber abordado las unidades propuestas en el diplomado de Linux y haber comprendido la base teórica y práctica para implementar soluciones bajo un ambiente GNU/Linux, el presente artículo profundiza la instalación del sistema Zentyal 6.2 que permitirá y facilitará la implementación y administración de servicios en una red establecida. Se detalla el desarrollo de las cinco (5) temáticas que relacionan solución en implementación de servicios en una infraestructura de IT: Temática 1 DHCP Server, DNS Server y controlador de dominio. Temática 2: Proxy no transparente. Temática 3: Cortafuegos. Temática 4: File Server y Print Server, finalmente la Temática 4: VPN.

2 ZENTYAL SERVER

2.1 DESCARGA

Antes de iniciar la instalación se debe de realizar la descarga el archivo ISO desde la URL <https://zentyal.com/es/comunidad/>

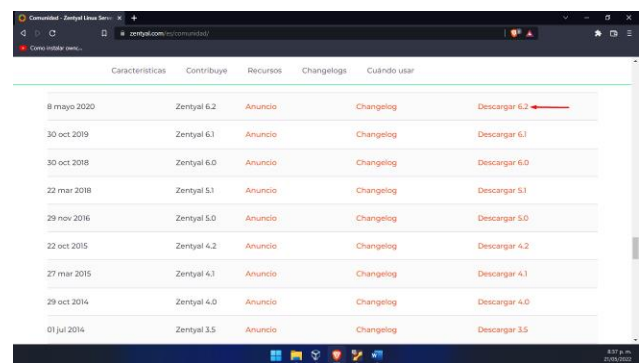


Imagen 1. Descarga de Zentyal Server

Se valida que la imagen .ISO de instalación del sistema quede en un repositorio donde se pueda instalar fácilmente desde la máquina virtual:

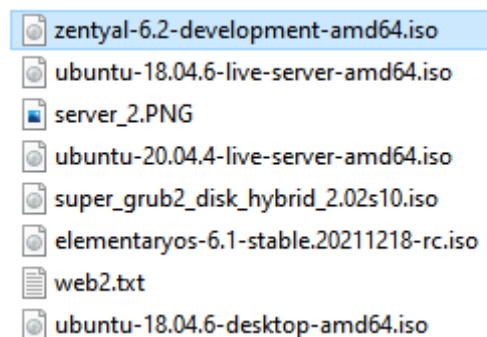


Imagen 2. Repositorio para instalar Zentyal

2.2 CREACIÓN MÁQUINA VIRTUAL

Se realiza la configuración de una nueva máquina virtual en la herramienta Oracle VM Virtual Box.

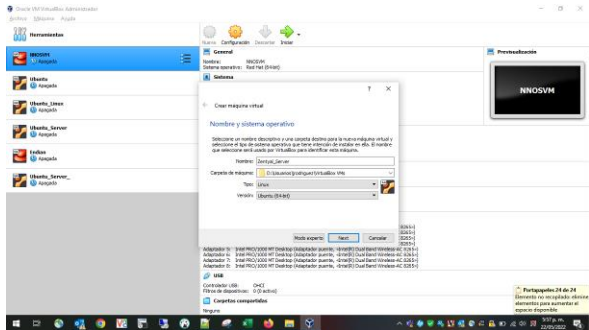


Imagen 3. Nueva máquina virtual – Zentyal Server

Se realiza configuración de características físicas para su correcto funcionamiento: Memoria 3072 MB, disco duro de 40 GB y adicional se configuran parámetros de red para su correcto funcionamiento. Adaptador 1 como adaptador puente para las conexiones externas y salida a internet y el Adaptador 2 como red interna, para la conexión hacia los equipos clientes con sistema operativo Ubuntu Desktop.

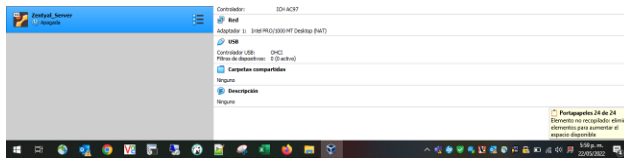


Imagen 4. Configuración exitosa máquina virtual – Zentyal Server

2.3 INSTALACIÓN ZENTYAL SERVER

Zentyal es un sistema operativo basado en GNU/Linux que facilita la gestión de los servicios de infraestructura IT como Servidor de Dominio, DHCP, DNS, Correo, Gateway, de Infraestructura, Mantenimiento, Actualizaciones y Soporte, este último para la versión comercial.

Creamos la máquina virtual Zentyal por medio de Virtual Box, la cual configuramos con la versión recomendada para el desarrollo de la actividad final (6.2), la red adaptador puente para la interfaz roja y la red interna para la interfaz verde.

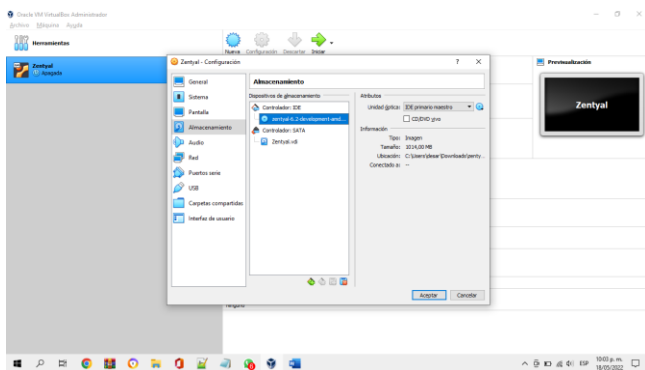


Imagen 5. Configuración de almacenamiento.

Seleccionamos el idioma español

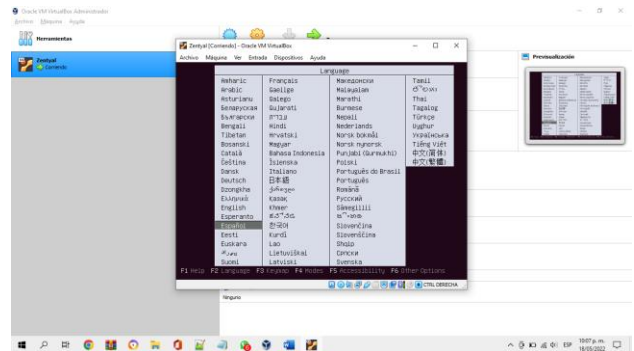


Imagen 6. Configuración de idioma.

Seleccionamos la primera opción para instalar Zentyal

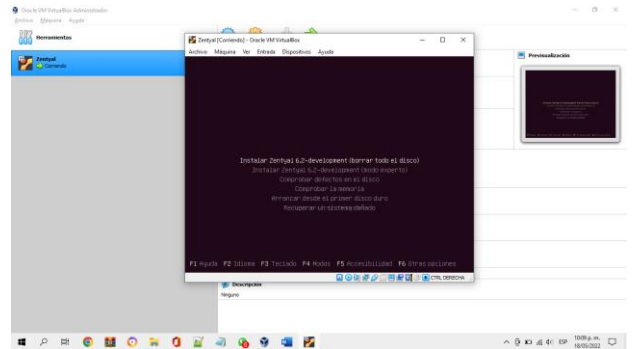


Imagen 7. Instalación Zentyal.

Seleccionamos el país o región

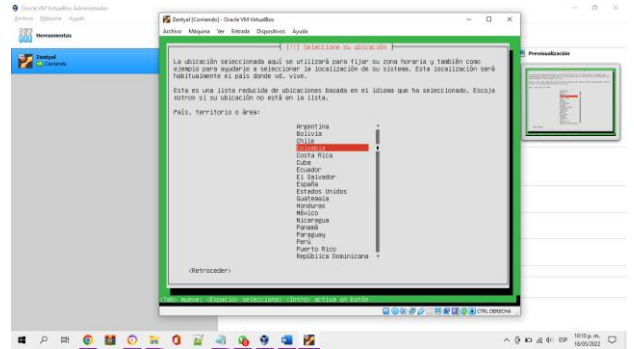


Imagen 8. País o región

En la configuración de red seleccionamos la interfaz de red primaria eth0

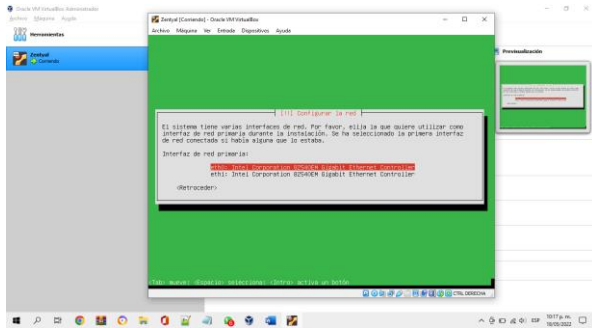


Imagen 9. Configuración de red

Configuramos el nombre de la máquina virtual

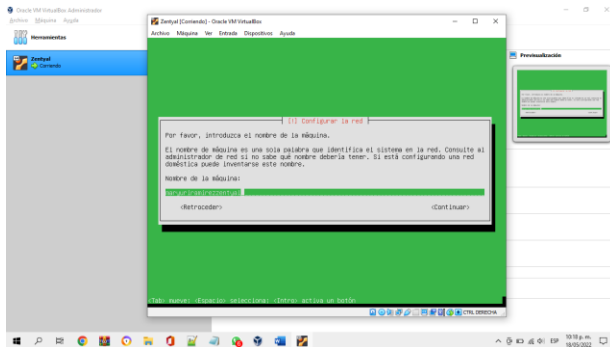


Imagen 10. Configuración del nombre de la máquina.

Configuramos el nombre de usuario para la cuenta

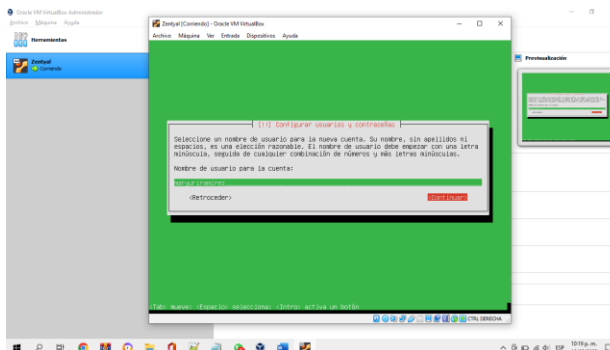


Imagen 11. Configuración nombre de usuario

Ingresamos la contraseña para el usuario

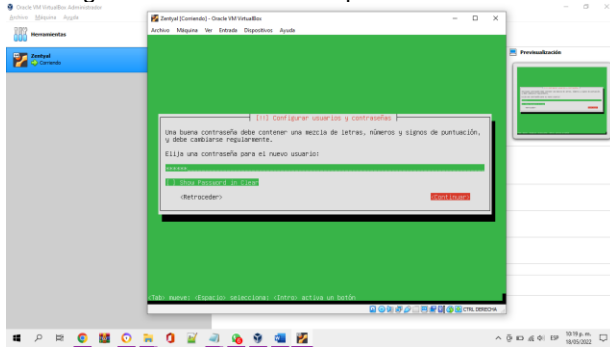


Imagen 12. Configuración contraseña usuario

Observamos que ha terminado la instalación de manera correcta y damos clic en continuar

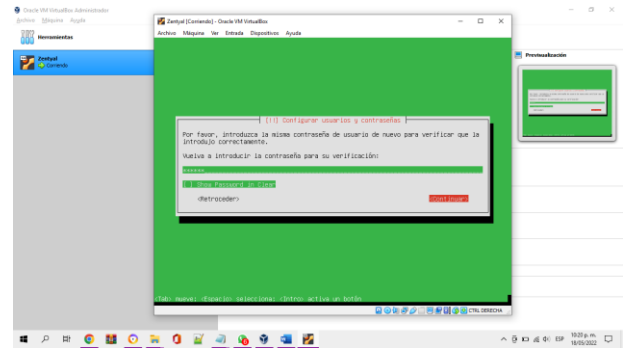


Imagen 13. Instalación terminada

Observamos Zentyal y ya podemos iniciar sesión

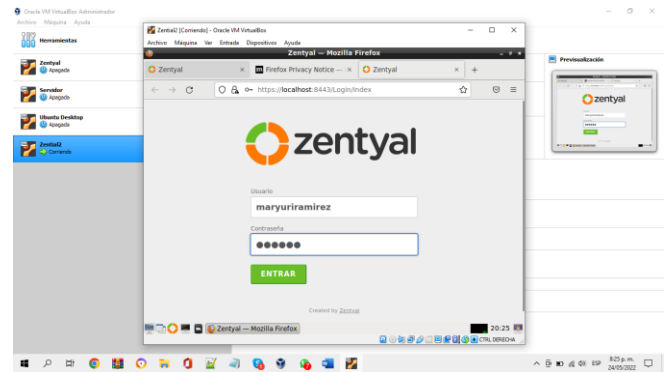


Imagen 14. Inicio Zentyal

3 TEMÁTICAS

- Temática 1 – DHCP Server, DNS Server y controlador de Dominio.
- Temática 2 – Proxy no transparente
- Temática 3 – Cortafuegos
- Temática 4 – File Server y Print Server
- Temática 5 – VPN

3.1 Temática 1 – DHCP Server, DNS Server y controlador de Dominio

Se realizará la implementación y configuración del acceso de una estación de trabajo con Ubuntu Desktop 20.04.4 LTS desde un usuario y contraseña, así como el registro de esta estación en los servicios de infraestructura IT de Zentyal 6.2

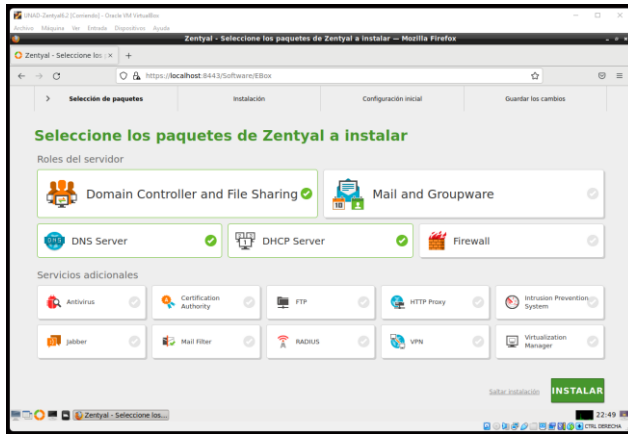


Imagen 15. Selección de los paquetes a instalar.

Se seleccionan los paquetes necesarios a instalar: Domain controller and file sharing, DNS Server y DHCP Server.

Para iniciar configuramos el tipo de controlador de dominio que necesitamos en este caso el servicio estará como controlador de dominio principal:

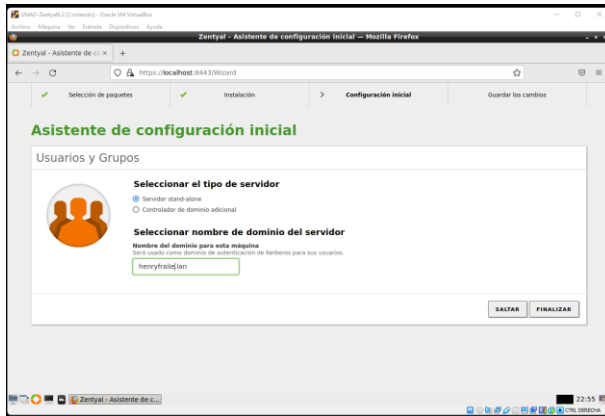


Imagen 16. Selección del tipo de domain controller.

Luego verificamos el estado de los servicios:



Imagen 17. Estado de los módulos.

Después ingresamos a usuarios y equipos para crear un usuario, para el ejemplo crearemos un usuario con permisos de administrador llamado mesa.servicio:



Imagen 18. Creación de usuario en el dominio con Zentyal.

A continuación, unimos la máquina virtual Ubuntu Desktop al dominio para esto lo primero que vamos a hacer es ejecutar el siguiente comando:

```
dig -t SRV _ldap._tcp.henryfrailan
```

Información obtenida:

Dominio: henryfrailan

Nombre del servidor Dominio: zentyalunad.henryfrailan

Ahora instalaremos y configuraremos unas librerías necesarias:

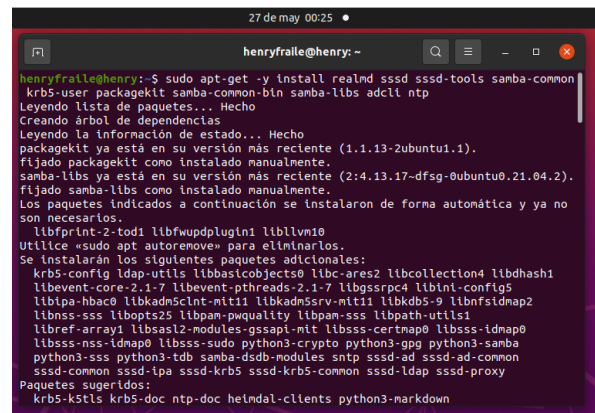


Imagen 19. Instalación de librerías necesarias.

Ahora configuramos la autenticación con Kerberos:

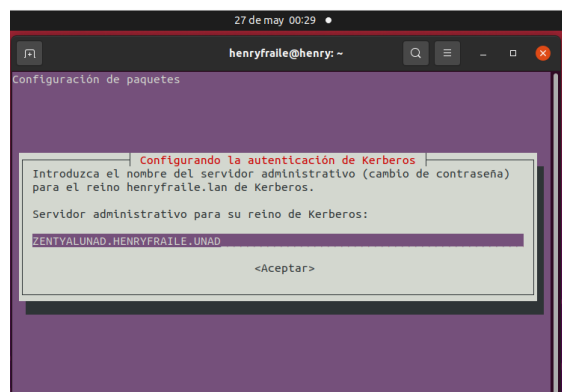


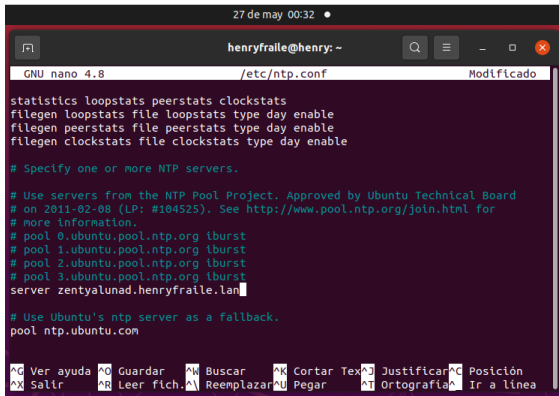
Imagen 20. Configuración autenticación con kerberos.

Ahora configuramos el servicio NTP hacia el controlador del dominio:

Modificamos con:

`sudo nano /etc/ntp.conf`

Dejando solo el servidor de zentyal como servidor NTP:



```
GNU nano 4.8 /etc/ntp.conf Modificado
statistics loopstats peerstats clockstats
filegen loopstats file loopstats type day enable
filegen peerstats file peerstats type day enable
filegen clockstats file clockstats type day enable

# Specify one or more NTP servers.

# Use servers from the NTP Pool Project. Approved by Ubuntu Technical Board
# on 2011-02-08 (LP: #104525). See http://www.pool.ntp.org/join.html for
# more information.
# pool.0.ubuntu.pool.ntp.org iburst
# pool.1.ubuntu.pool.ntp.org iburst
# pool.2.ubuntu.pool.ntp.org iburst
# pool.3.ubuntu.pool.ntp.org iburst
server zentyalunad.henryfraile.lan

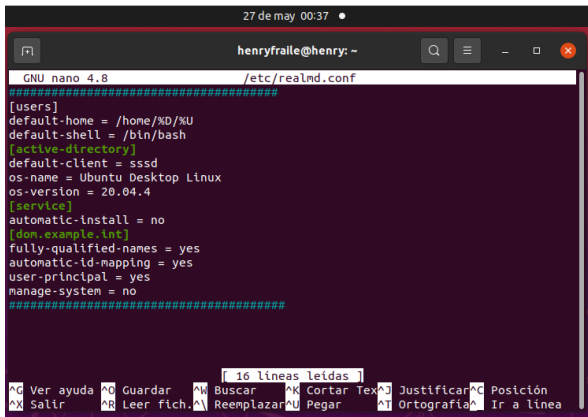
# Use Ubuntu's ntp server as a fallback.
pool ntp.ubuntu.com
```

Imagen 21. Configuración de servicio NTP.

Unimos el equipo desktop al dominio:

Editamos el siguiente archivo:

`sudo nano /etc/realmd.conf`



```
GNU nano 4.8 /etc/realmd.conf
[users]
default-home = /home/%D/%U
default-shell = /bin/bash
[active-directory]
default-client = sssd
os-name = Ubuntu Desktop Linux
os-version = 20.04.4
[service]
automatic-install = no
[dom.example.int]
fully-qualified-names = yes
automatic-id-mapping = yes
user-principal = yes
manage-system = no
```

Imagen 22. Configuración parámetros active directory

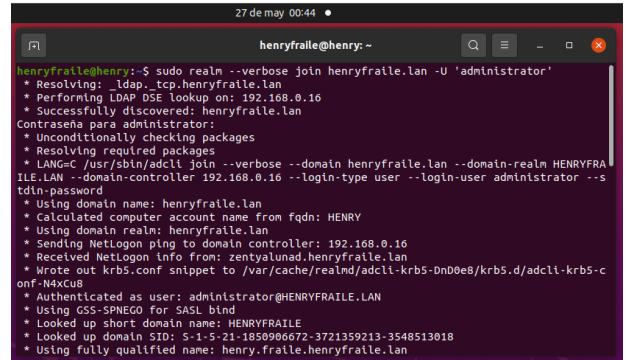
Se inicializa comunicación kerberos solicitando tickets con knit.

Ejecutar en una terminal:

`sudo kinit administrator`

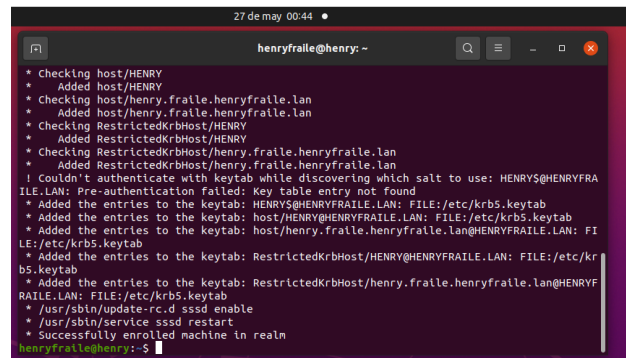
Luego unimos la maquina al dominio con el siguiente comando:

`sudo realm --verbose join henryfraile.lan -U 'administrator'`



```
henryfraile@henry:~$ sudo realm --verbose join henryfraile.lan -U 'administrator'
* Resolving: ldap_tcp.henryfraile.lan
* Performing LDAP DSE lookup on: 192.168.0.16
* Successfully discovered: henryfraile.lan
Contraseña para administrator:
* Unconditionally checking packages
* Resolving required packages
* LANG=C /usr/sbin/adjcli join --verbose --domain henryfraile.lan --domain-realm HENRYFR
ILE.LAN --domain-controller 192.168.0.16 --login-type user --login-user administrator --s
tdln-password
* Using domain name: henryfraile.lan
* Calculated computer account name from fqdn: HENRY
* Using domain realm: henryfraile.lan
* Sending Netlogon ping to domain controller: 192.168.0.16
* Received NetLogon info from: zentyalunad.henryfraile.lan
* Wrote out krb5.conf snippet to /var/cache/realmd/adjcli-krb5-dn00e8/krb5.d/adjcli-krb5-c
onf-N4xCu8
* Authenticated as user: administrator@HENRYFRRAILE.LAN
* Using GSS-SPNEGO for SASL bind
* Looked up short domain name: HENRYFRRAILE
* Looked up domain SID: S-1-5-21-1850906672-3721359213-3548513018
* Using fully qualified name: henry.fraile.henryfraile.lan
```

Imagen 23. Uniendo ubuntu desktop al dominio.



```
henryfraile@henry:~$
* Checking host/HENRY
* Added host/HENRY
* Checking host/henry.fraile.henryfraile.lan
* Added host/henry.fraile.henryfraile.lan
* Checking RestrictedKrbHost/HENRY
* Added RestrictedKrbHost/HENRY
* Checking RestrictedKrbHost/henry.fraile.henryfraile.lan
* Added RestrictedKrbHost/henry.fraile.henryfraile.lan
! Couldn't authenticate with keytab while discovering which salt to use: HENRY5@HENRYFR
AILE.LAN: Pre-authentication failed: Key table entry not found
* Added the entries to the keytab: HENRY5@HENRYFRRAILE.LAN: FILE:/etc/krb5.keytab
* Added the entries to the keytab: host/HENRY@HENRYFRRAILE.LAN: FILE:/etc/krb5.keytab
* Added the entries to the keytab: host/henry.fraile.henryfraile.lan@HENRYFRRAILE.LAN: FI
LE:/etc/krb5.keytab
* Added the entries to the keytab: RestrictedKrbHost/HENRY@HENRYFRRAILE.LAN: FILE:/etc/k
rb5.keytab
* Added the entries to the keytab: RestrictedKrbHost/henry.fraile.henryfraile.lan@HENRYF
RAILE.LAN: FILE:/etc/krb5.keytab
* /usr/sbin/update-rc.d sssd enable
* /usr/sbin/service sssd restart
* Successfully enrolled machine in realm
henryfraile@henry:~$
```

Imagen 24. Uniendo ubuntu desktop al dominio.

Verificamos que el equipo aparezca en el listado de equipos unidos al controlador de dominio:

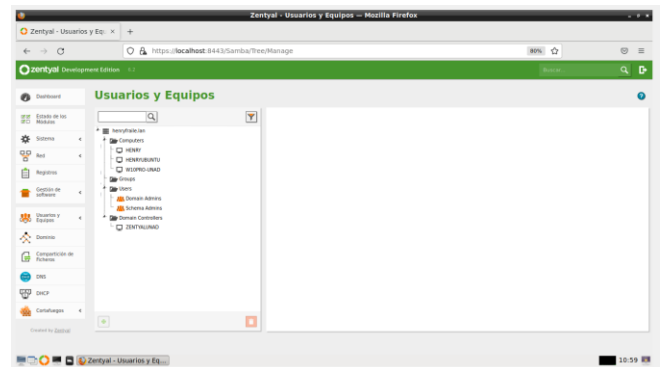


Imagen 25. Verificando el ubuntu en zentyal server.

Cerramos sesión en Ubuntu Desktop e iniciamos sesión con el usuario creado en zentyal (mesa.servicio)

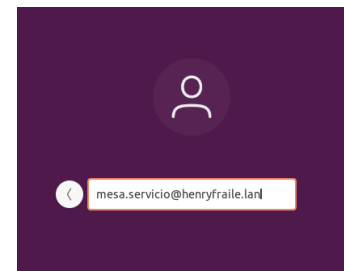


Imagen 26. Iniciando sesión en el dominio.

Iniciamos sesión correctamente con el usuario creado en el servidor de Zentyal y su controlador de dominio:



Imagen 27. Inicio de sesión exitoso.

3.2 Temática 2 – Proxy no transparente

Por medio del desarrollo de la presente temática se va a implementar el servicio de un Proxy no transparente, por medio del cual se controlarán los servicios de conectividad a Internet desde el Zentyal Server al equipo cliente, en esta práctica, al sistema Ubuntu Desktop.

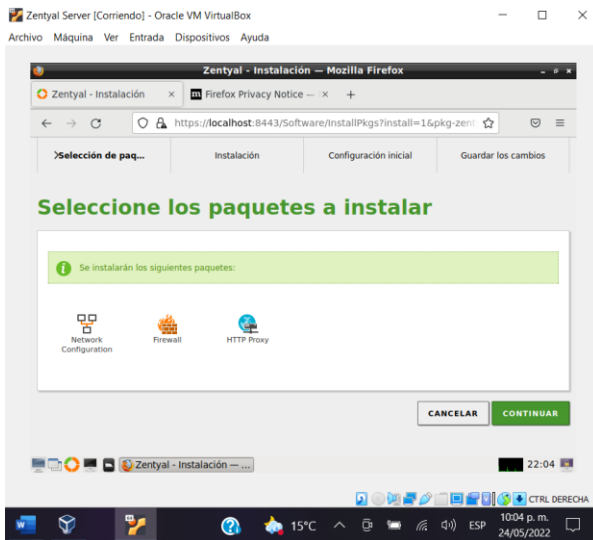


Imagen 28. Selección de los paquetes por instalar

En la configuración de las interfaces de red, se asigna la eth0 como externa, ya que hace referencia a la conexión a internet; y la eth1 se asigna como interna, con la finalidad de establecer la comunicación con el equipo cliente:

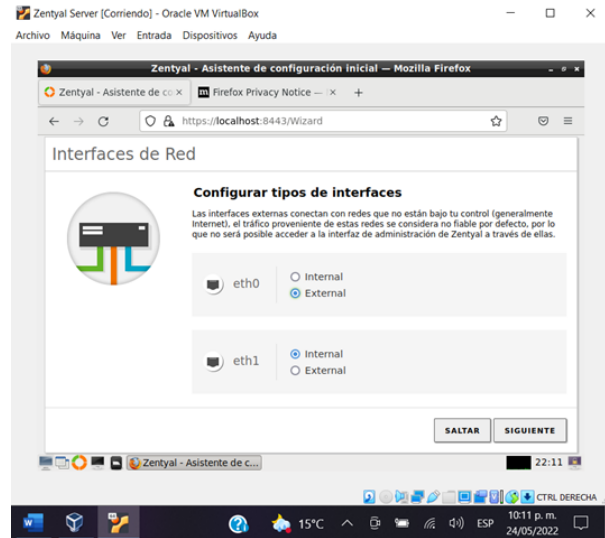


Imagen 29. Configuración de los tipos de interfaces

A continuación, se configuran las direcciones IP de cada interface de red; en lo correspondiente a la eth0, se selecciona el método DHCP, con la finalidad de que la IP sea asignada automáticamente; y para la eth1, se selecciona el método estático, en donde se va a asignar una IP dentro de un rango diferente al de la eth0:

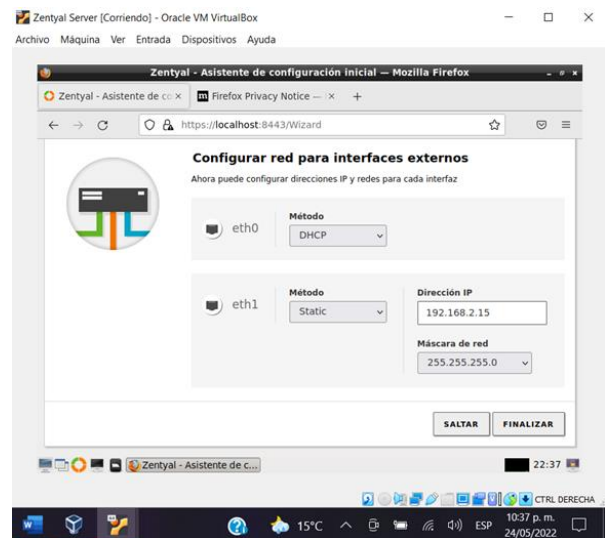


Imagen 30. Configuración de la red para interfaces internas

Como paso siguiente, se configura la red del equipo cliente, Ubuntu Desktop, con la idea de proporcionarle una IP en el rango en el que se encuentra el Zentyal Server, en donde la dirección se establecerá dentro de este rango y la puerta de enlace correspondería a la IP estática del Zentyal; como DNS, se va a hacer empleo del servidor de Google:

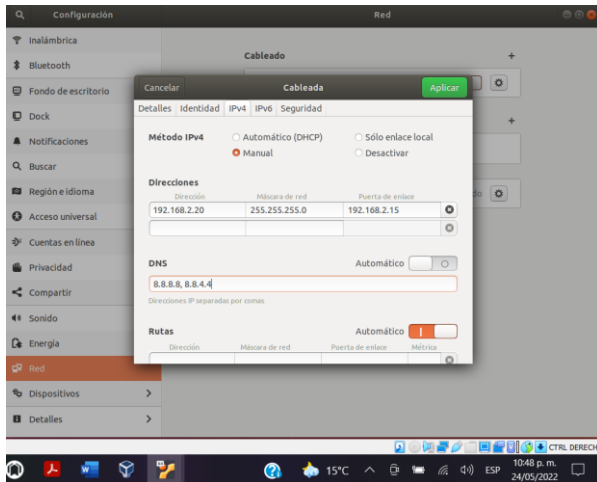


Imagen 31. Configuración de Red del Ubuntu Desktop

Una vez realizada la configuración en el equipo cliente, se verifica la conexión a internet

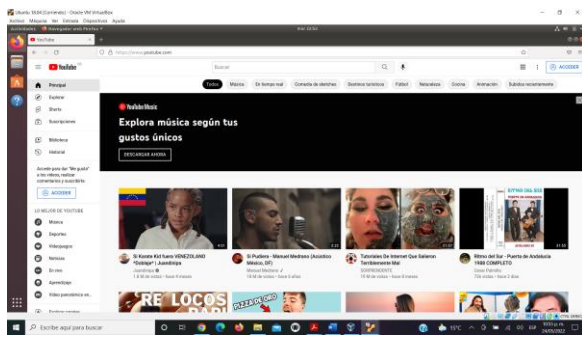


Imagen 32. Conexión a Internet en Ubuntu Desktop

Ahora, con el propósito de simplificar y facilitar la gestión de la configuración de la red por medio del proxy no transparente, se procede a crear un objeto, el cual representará al grupo de elementos que la componen:

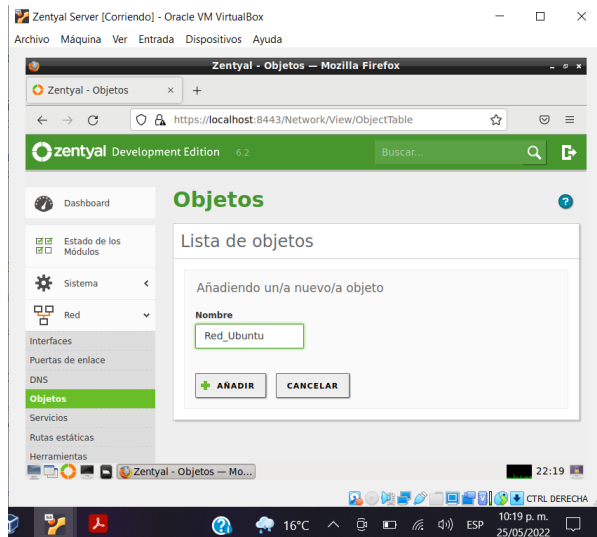


Imagen 33. Creación de Objetos en Zentyal

Ahora se crea un nuevo miembro para el objeto de red; para esto, se le asigna un nombre y la dirección IP del equipo cliente:

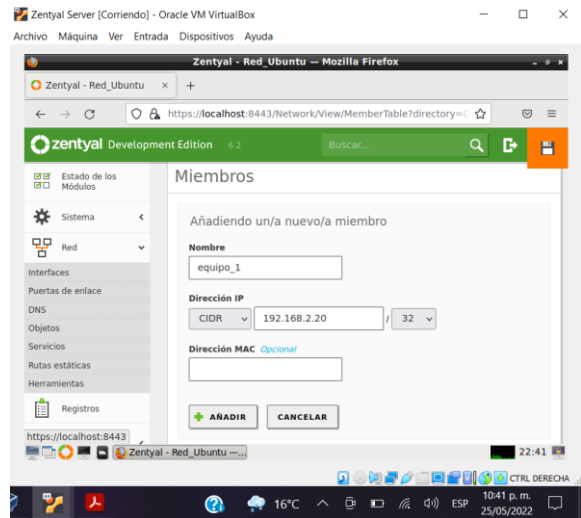


Imagen 34. Creación de Miembros en Zentyal

Se evidencia el mensaje de validación sobre el miembro añadido:

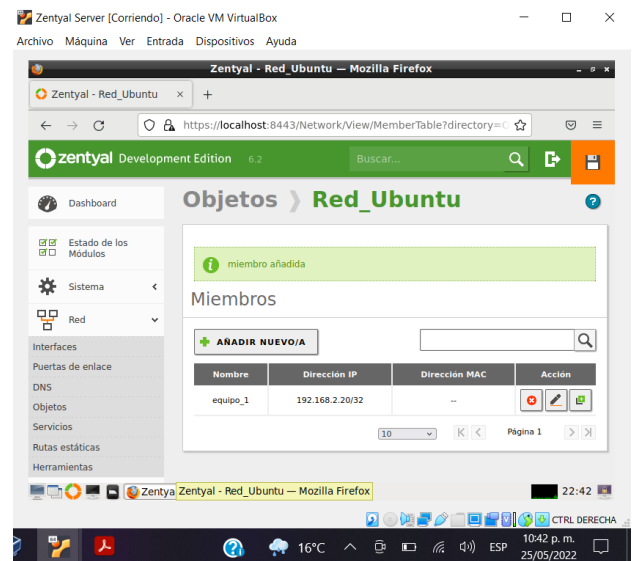


Imagen 35. Validación de la Creación del Miembro en Zentyal

Una vez creado el objeto y el miembro en Zentyal, se realiza la configuración del Proxy; en donde, con la idea de poder utilizar el servicio como un Proxy No Transparente, se deja desmarcada la casilla de Proxy Transparente, y se asigna el puerto por donde se filtrará la salida de los servicios de conectividad a Internet:

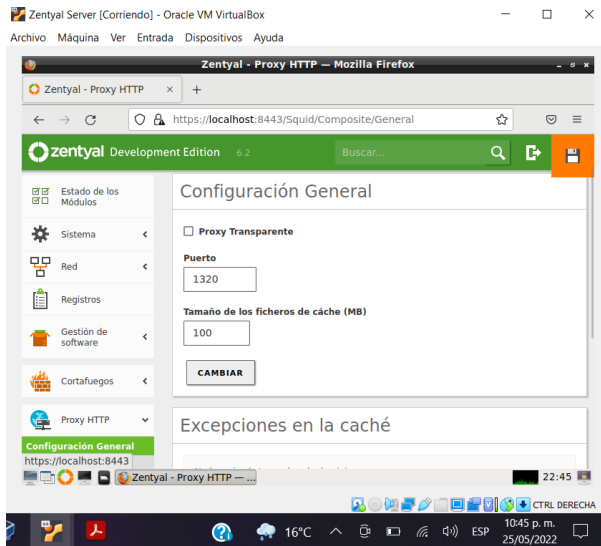


Imagen 36. Configuración de Proxy No Transparente

Se procede luego con la configuración de las Reglas de Acceso para el objeto que se ha creado; en este caso, se edita la regla que ya se encuentra ahí establecida:

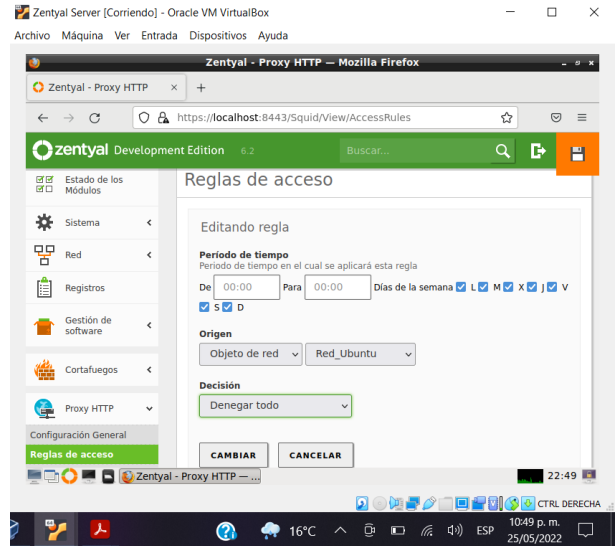


Imagen 38. Edición de la Regla de Acceso

Se aplican los cambios realizados

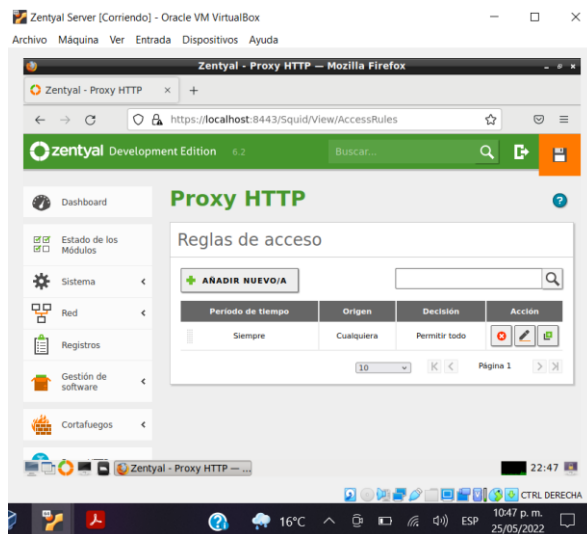


Imagen 37. Reglas de Acceso en Zentyal

En esta edición, se establece como origen al objeto de red creado anteriormente (Red_Ubuntu), y como decisión, con la finalidad de demostrar el control de acceso a la conectividad a internet, se va a denegar el acceso a éste:

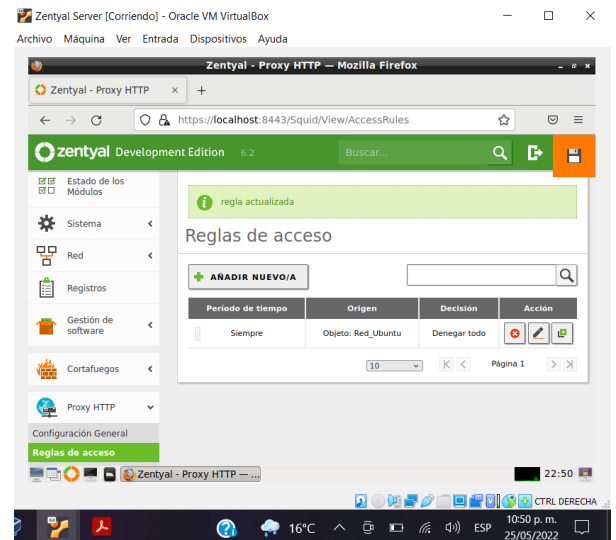


Imagen 39. Verificación de las Cambios Realizados a la Regla de Acceso

Como paso importante para tener en cuenta, es fundamental guardar los cambios realizados hasta el momento, para esto, se dirige a la parte superior derecha y se da click sobre el icono de guardar (icono de Diskette):

3.3 Temática 3 – Cortafuegos

En esta temática se pretende implementar y configurar la restricción de la apertura de sitios o portales Web de entretenimiento y redes sociales, evidenciando las reglas y políticas creadas. Para esto, después de instalado el servidor se instala las herramientas necesarias del Zentyl

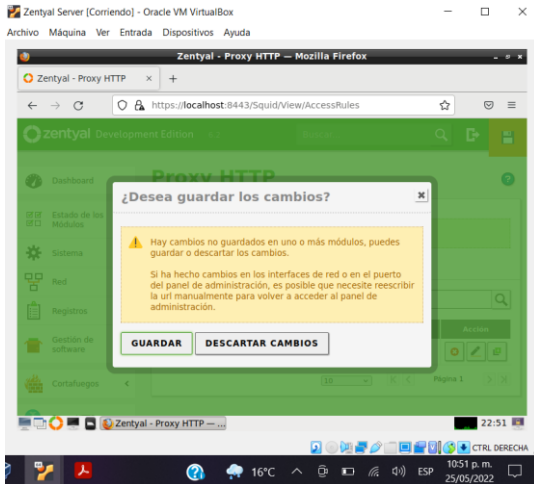


Imagen 40. Guardar Cambios en Zentyl

Ahora, se configura el Proxy de la Red en el equipo cliente, Ubuntu Desktop, en donde se le asigna la dirección IP del servidor Zentyl con el puerto que ya se estableció para que cumpla con este servicio:

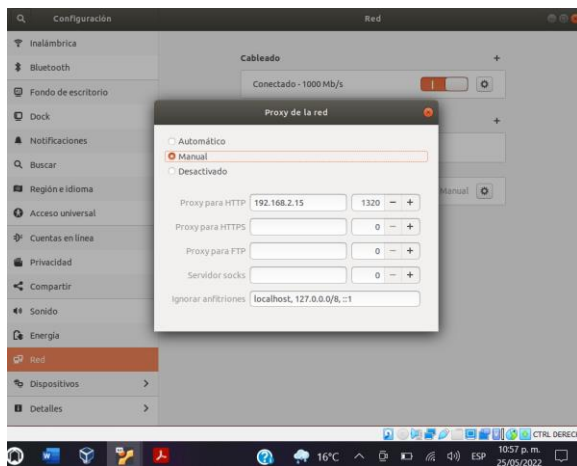


Imagen 41. Configuración del Proxy de la Red en Ubuntu Desktop

Para finalizar, se verifica la navegabilidad en el equipo cliente, accediendo a un sitio web determinado, y comprobando el bloqueo a la conectividad por parte del Proxy:

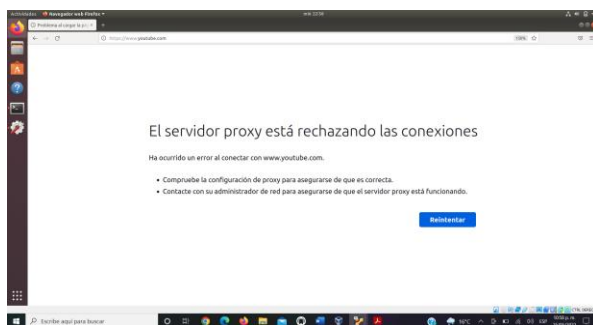


Imagen 42. Validación del Servicio de Proxy No Transparente en el Equipo Cliente

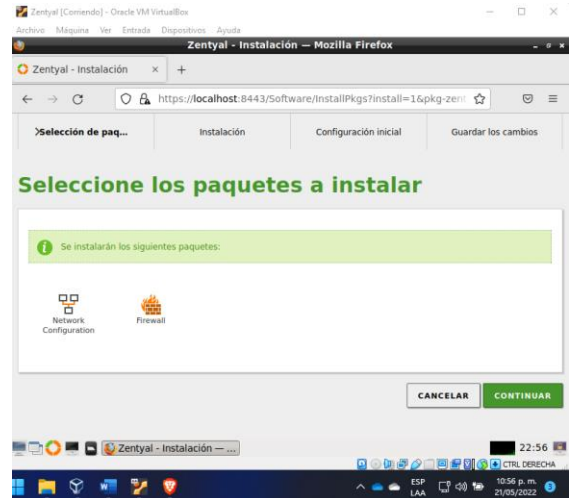


Imagen 43. Paquetes por instalar

Se selecciona el método de IP de cada tarjeta de red, en este caso la eth0 queda con DHCP, es decir, asignación de IP automática y la eth1 queda con Static y se le asigna una IP con un rango de IP diferente a la que da el servicio de internet por la eth0

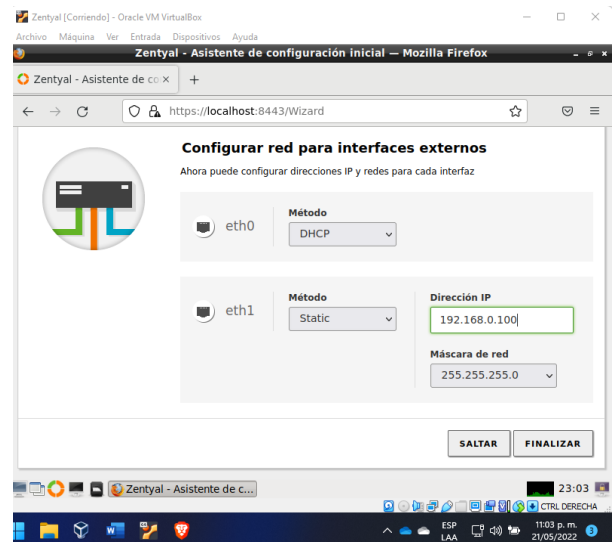


Imagen 44. Configuración interfaces de red

Se agrega a la red una máquina que tiene instalada la distribución Ubuntu 18.04 Desktop con una IP con el rango del servidor Zentyl, la puerta de enlace es la dirección IP de la tarjeta de red interna del servidor Zentyl y DNS de Google

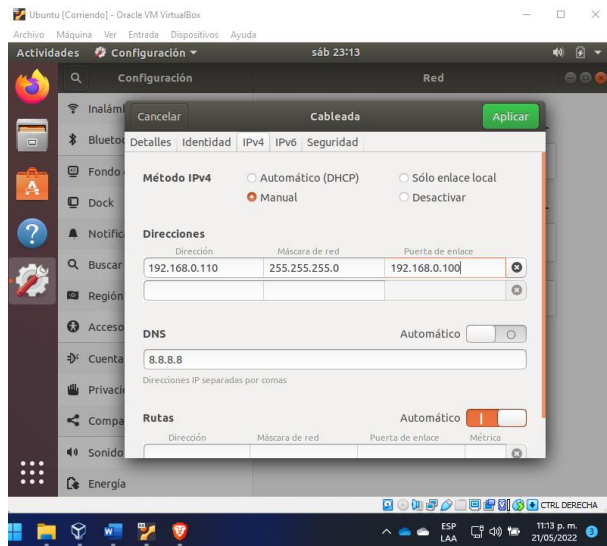


Imagen 25. Configuración red equipo cliente

Se evidencia que el equipo ya cuenta con navegación a internet y se ingresa a la red social Facebook

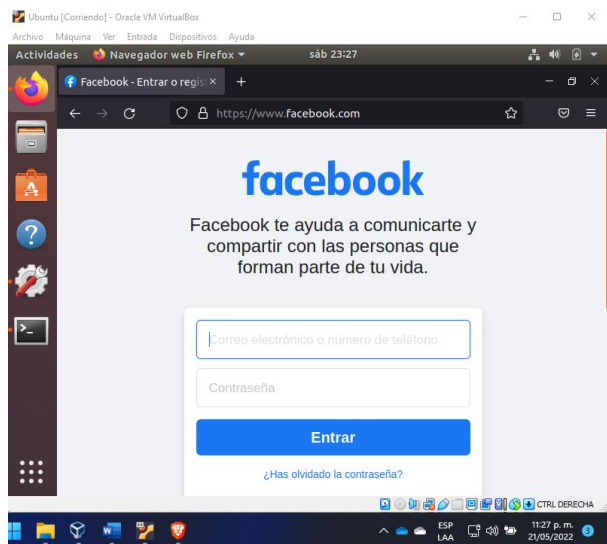


Imagen 46. Validación navegación

Teniendo en cuenta que las reglas del Firewall que trabaja este servidor pueden ser por IP y se pueden almacenar en rangos como objetos creados desde la red. Se crea el objeto Facebook

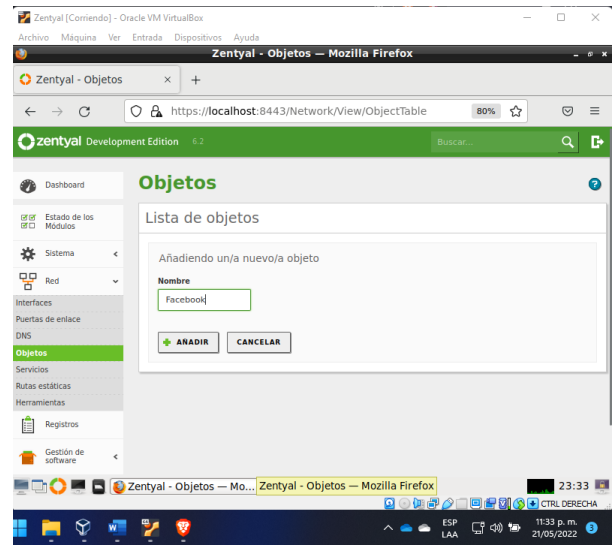


Imagen 47. Creación de objetos

Se crean los miembros los miembros que son los mismos rangos de las IP descubiertas del dominio a bloquear, en este caso Facebook, mediante ping

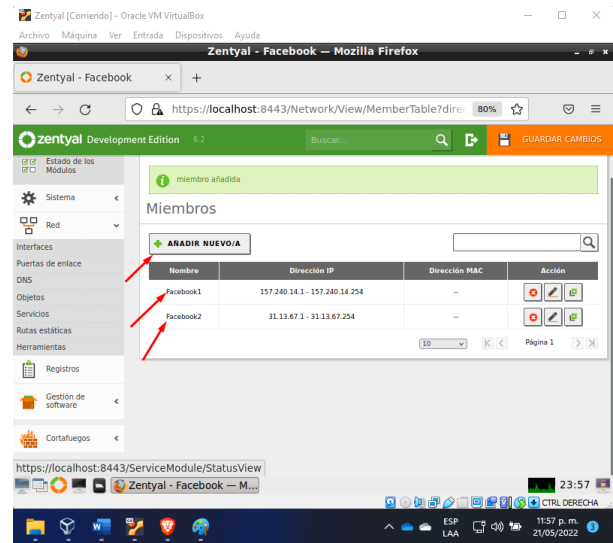


Imagen 48. Creación de miembros

Se configura la regla de filtrado para redes internas, donde se le deniega el acceso al objeto creado llamado Facebook por medio del servicio TCP

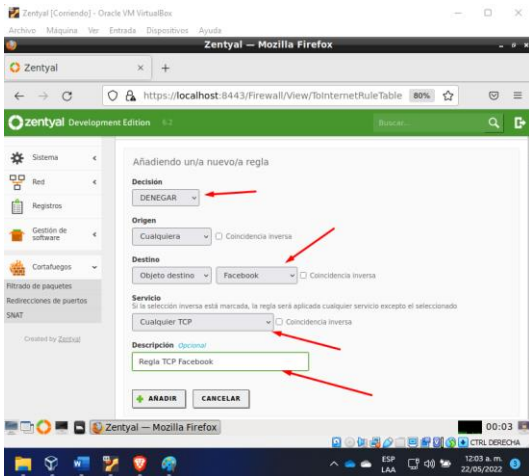


Imagen 49. Bloqueo Facebook servicio TCP

También, le deniega el acceso al objeto creado llamado Facebook por medio del servicio HTTP.

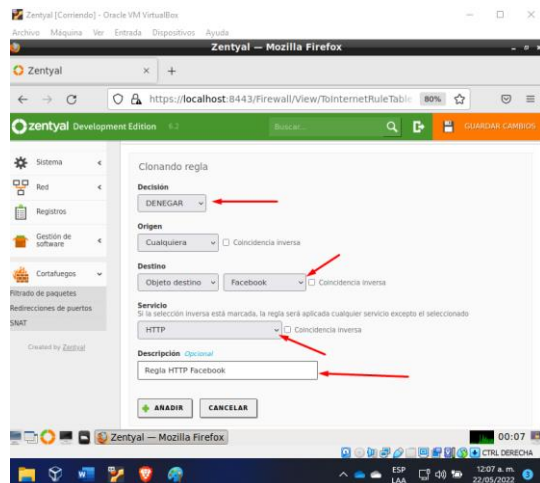


Imagen 50. Bloqueo Facebook servicio HTTP

Por último, le deniega el acceso al objeto creado llamado Facebook por medio del servicio HTTPS

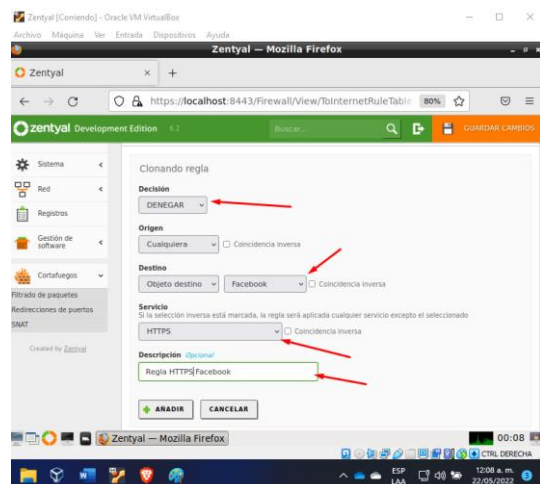


Imagen 53. Bloqueo Facebook servicio HTTPS

Se intenta ingresar a la red social Facebook, para que los resultados sean reales, se recomienda borrar el caché del navegador previamente.

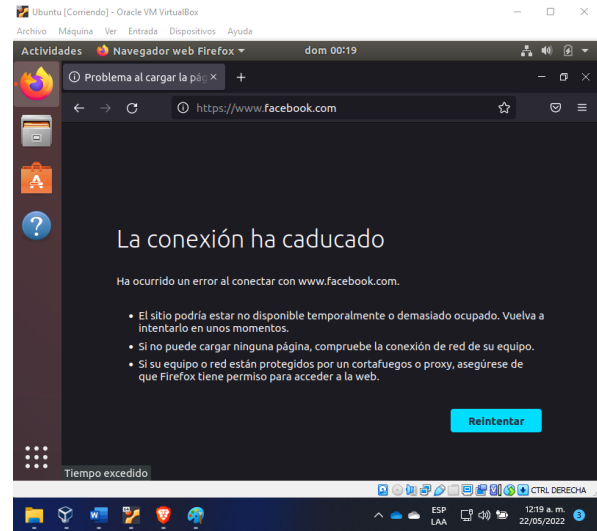


Imagen 52. Prueba ingreso a red social

3.4 Temática 4 – File Server y Print Server

Procedemos a instalar el servicio “Domain Controller and File Sharing”

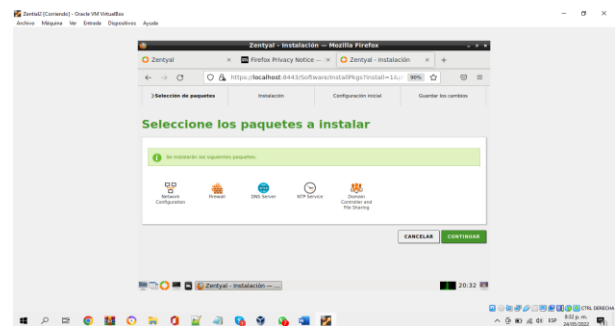


Imagen 53. Instalación del servicio Domain

Configuramos la Interface de red de tipo Internal por el métodoStatic

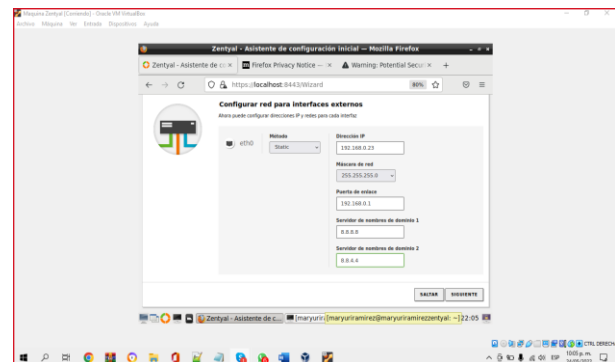


Imagen 55. Configuración de la interface

Activamos el módulo de controlador de dominio y compartición de archivos

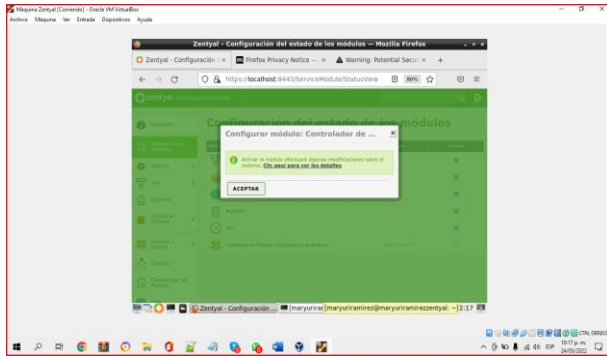


Imagen 56. Activación del módulo de controlador

Creamos los grupos y usuarios que consideramos necesarios

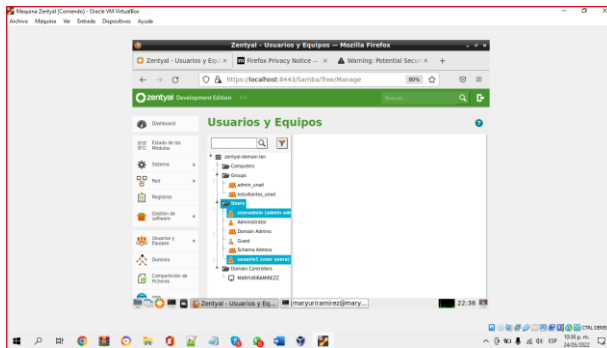


Imagen 57. Evidencia creación de grupos

Añadimos una nueva compartición de ficheros

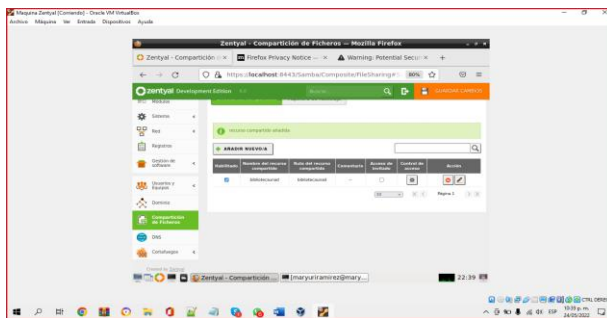


Imagen 58. Compartición de ficheros

Configuramos el control de acceso (Usuario/Grupo - Permiso)

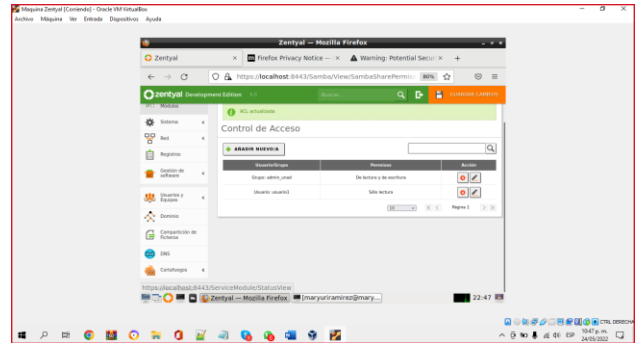


Imagen 59. Configuración control de acceso

Instalamos el servidor Samba (permite a las distribuciones de Linux/Ubuntu compartir archivos e impresoras con cualquier otro dispositivo conectado a la red.)

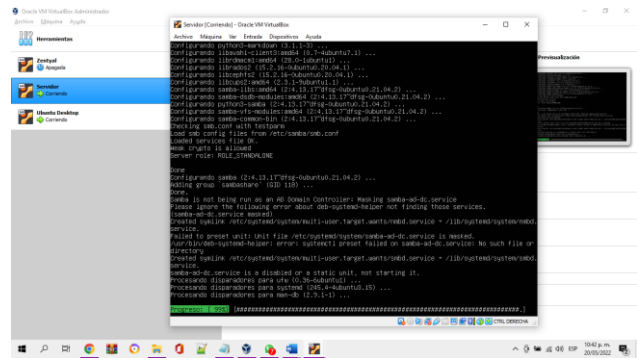


Imagen 60. Instalación Servicio Samba

Accedemos al archivo de configuración smb.conf, agregamos el parámetro security=user y en la etiqueta printers le ponemos yes a los parámetros browseable y guest ok

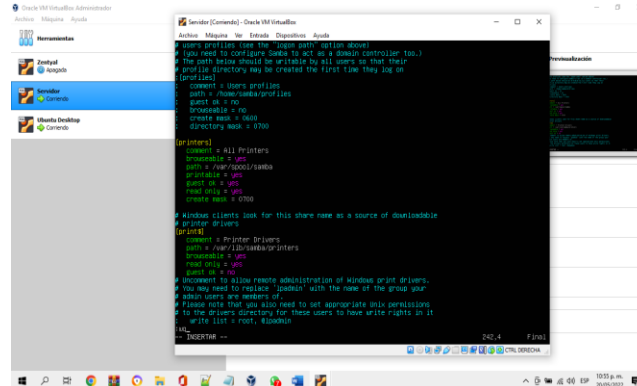


Imagen 61. Archivo configuración Samba

Reiniciamos el servidor de samba para aplicar todos los cambios

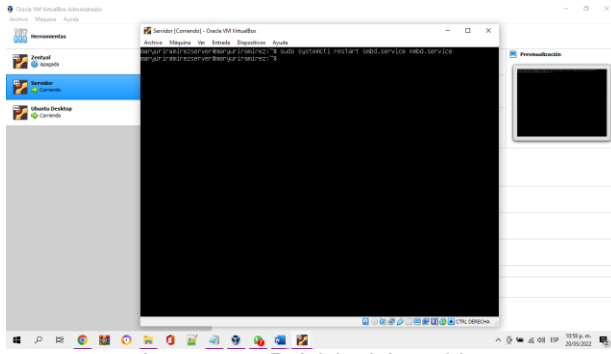


Imagen 62. Reinicio del servidor

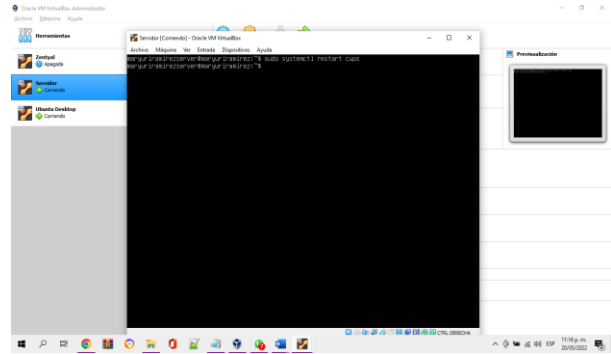


Imagen 23. Reinicio del servicio CUPS

Instalamos el servidor CUPS (Sistema de impresión que permite configurar un equipo como servidor de impresión en Linux, puede administrar impresoras desde ordenadores cliente)

Ingresamos a Ubuntu desktop y configuramos la conexión al servidor mb://192.168.0.23/

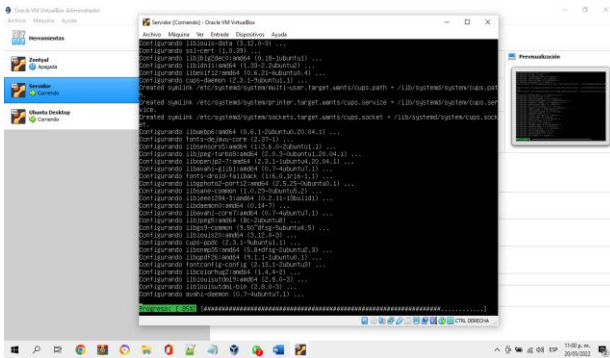


Imagen 21. Instalación del servicio CUPS

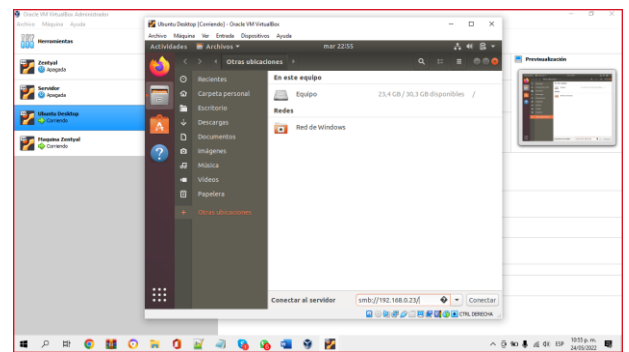


Imagen 24. Conexión al servidor

Una vez conectados podemos observar la carpeta compartida "bibliotecaunad".

Accedemos al archivo de configuración cups.conf, reemplazamos Listen localhost:631 por Port 631 y agregamos el parámetro Allow all

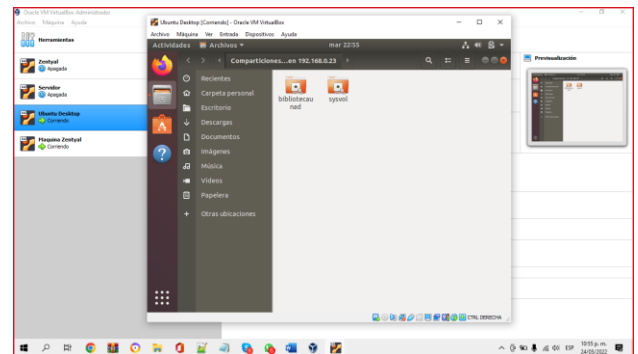


Imagen 25. Carpeta comprimida

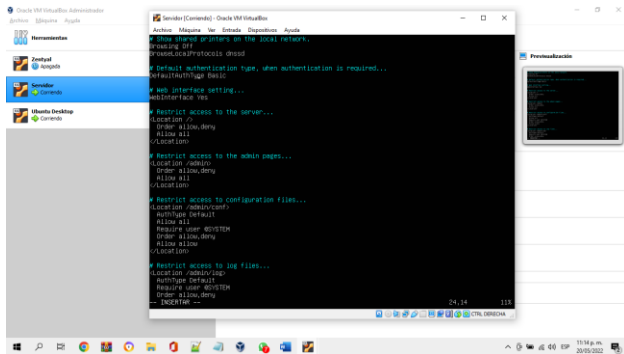


Imagen 22. Archivo configuración CUPS

Para acceder a la carpeta ingresamos usuario y contraseña.

Reiniciamos el servicio de impresión CUPS para que tome los cambios realizados

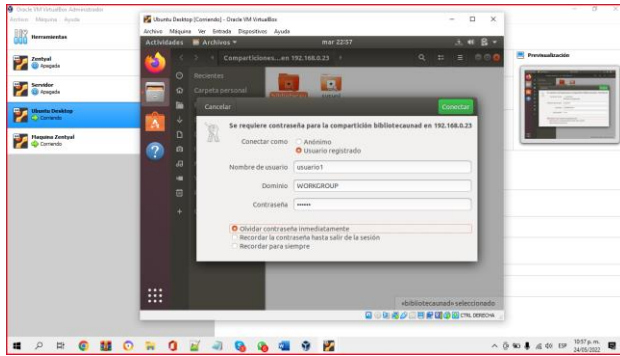


Imagen 26. Ingreso de usuarios

Podremos realizar acciones de acuerdo con los permisos que tenga asignado el usuario.

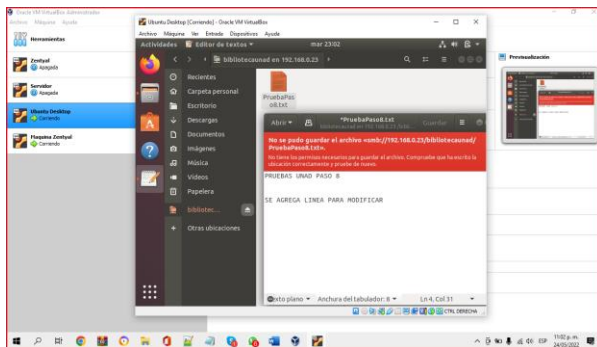


Imagen 27. Evidencia permisos de usuarios

Abrimos el navegador e ingresamos la ip del Ubuntu server con el puerto 631 donde podemos administrar el print server.

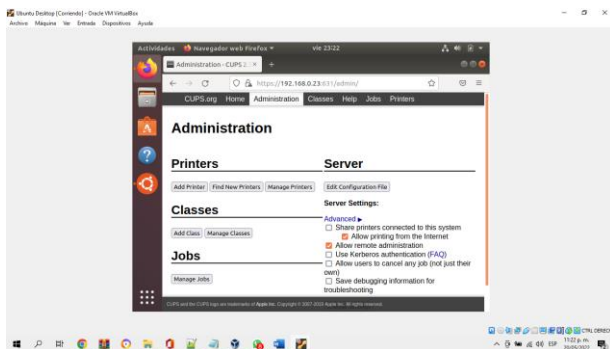


Imagen 28. Servicio Print Server

En la configuración de dispositivos añadimos la nueva impresora CUPS

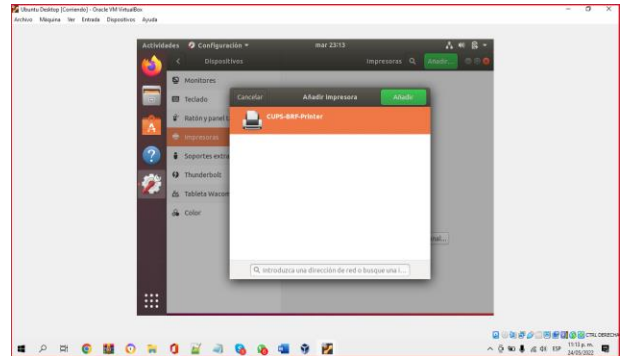


Imagen 29. Añadir una nueva impresora CUPS

Una vez añadida la impresora podemos observarla disponible

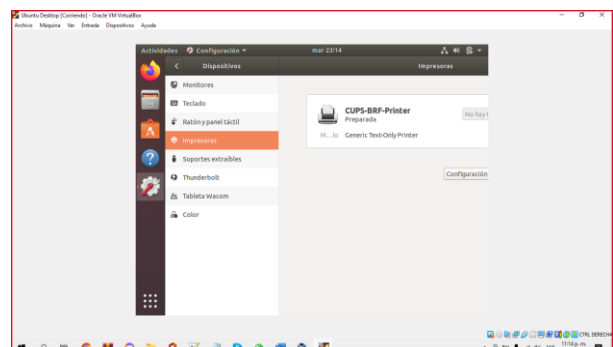


Imagen 30. Observamos la impresora CUPS

3.5 Temática 5 – VPN

Después de autenticarnos exitosamente en Zentyal server URL <https://localhost:8443>, en la opción de configuración inicial podemos identificar y habilitar los servicios necesarios para implementar un servidor de VPN. Se seleccionan principalmente: Certification Authority y VPN:

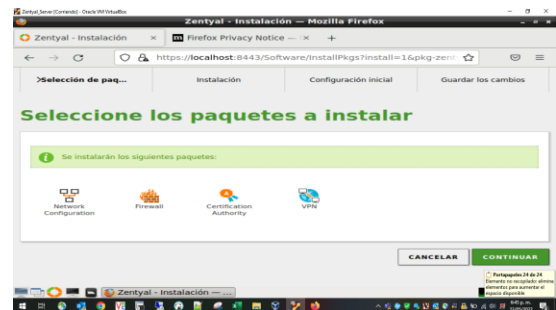


Imagen 31. Paquetes Por Instalar para VPN

La herramienta de gestión nos permite realizar la configuración de tipo de interfaces de red. Se opta por dejar la interfaz eth0 para la red externa y la interfaz eth1 para la red interna y que pueda comunicarse con el equipo cliente, Ubuntu desktop. Cuando se selecciona el tipo de red, permite configurar de una vez el direccionamiento, para lo cual dejamos la interfaz eth0 para obtener direccionamiento dinámico por DHCP y la

interfaz eth1, método static, configuramos un segmento de red 192.168.1.100/24:



Imagen 32. Asistente configuración de interfaces

Posteriormente desde la ventana principal donde se puede visualizar el dashboard se procede a iniciar la configuración:

Para realizar la configuración de un servidor VPN en Zentyal 6.2, se ingresa al Dashboard, en el panel izquierdo, se observan los módulos que se agregaron, inicialmente se da clic en la opción VPN y a continuación clic en la opción Servidores:

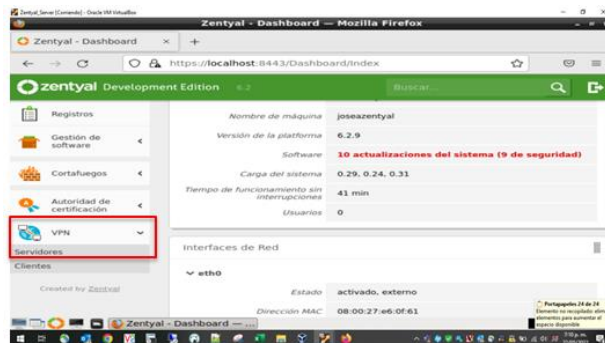


Imagen 33. Módulo VPN Zentyal

Antes de realizar la configuración, el mismo asistente solicita que se debe contar con un certificado de autenticación, por lo cual se configura certificado tanto para servidor como para cliente. Al dar clic en Servidores VPN, se puede dar clic en el módulo autoridad de certificación



Imagen 34. Módulo Autoridad de certificado

Para el servidor, se crea certificado de autoridad. Para lo cual es obligatorio dar un nombre de organización, DPLinux y configurar tiempo donde expirará el certificado, para el proyecto 365 días. Si bien los demás campos no son obligatorios también se configuran, Código de país, ciudad y estado:

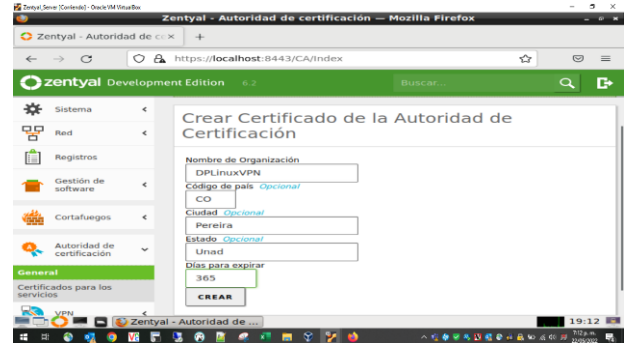


Imagen 35. Crear certificado de autenticidad

Automáticamente, se puede visualizar el certificado, identificando que Zentyal actúa como una Autoridad de Certificación.

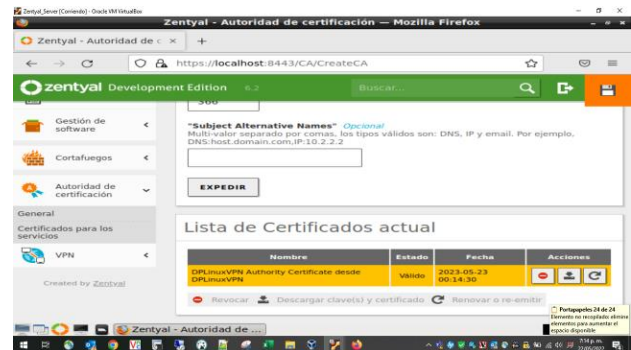


Imagen 36. Lista certificados Actual

Una vez se configuran certificados, se procede a ajustar la configuración del servidor VPN en Zentyal mediante la opción Crear un nuevo servidor. El único parámetro que se requiere es introducir un nombre de servidor. Zentyal configura los demás parámetros y valores de forma automática, sin embargo, se pueden ajustar dando clic en el icono de configurar:

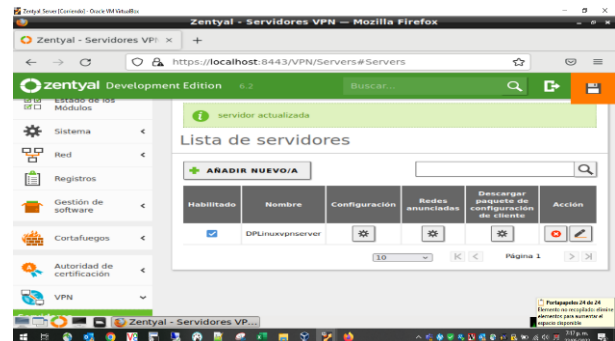


Imagen 37 Lista de servidores

Se da clic en la opción de Configuración. Allí se ajusta el puerto donde se escucharán las conexiones, por defecto es el puerto 1194 y se deja el segmento de red por default para asignar a los clientes cuando se conecten a la red privada: 192.168.160.0/24



Imagen 38 Configuración de servidor

Luego se configura el cliente VPN. La forma más sencilla de configurar un cliente VPN es utilizando los bundles de Zentyal, paquetes de instalación que incluyen el archivo de configuración de VPN específico para cada usuario y, opcionalmente, un programa de instalación.

Los bundles están disponibles en la tabla que aparece en VPN / Servidores, pulsando el icono de la columna Descargar bundle del cliente. Se pueden crear bundles para clientes Windows, Mac OS y Linux. En nuestro escenario, se realizará la creación para el sistema operativo Linux, y al crear el bundle se seleccionan aquellos certificados que se van a dar al cliente y se establece la dirección externa del servidor a la cual los clientes VPN se deben conectar.

Se debe identificar el nombre de certificado, se asocia al nombre de usuario del equipo con Sistema operativo Ubuntu Desktop, queda josearodriguez. Se configura tiempo para expirar de 1 año (365 días) y se configura la dirección IP del servidor VPN:

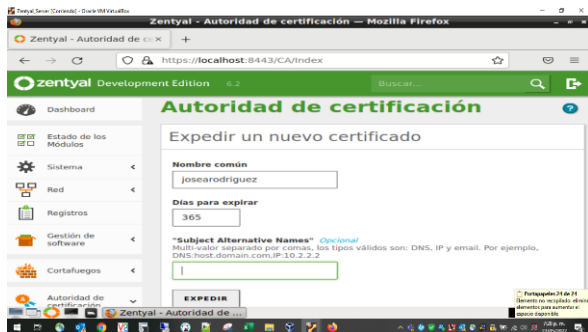


Imagen 39 Expedir certificado cliente

Se valida el direccionamiento en las dos interfaces de Zentyal 6.2, tanto la red externa con la IP 192.618.1.9 que la da por DHCP el Cable modem Wifi, y la dirección interna en la interfaz eth1 192.168.2.100:

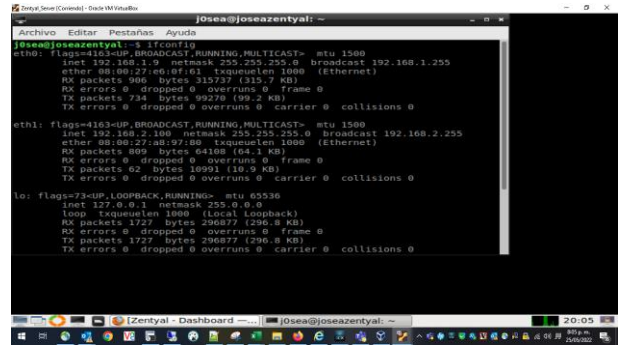


Imagen 40 Validar direccionamiento Zentyal

Se descarga el archivo de certificado para vpn del equipo cliente y se copia en este caso al equipo con sistema operativo Ubuntu Desktop

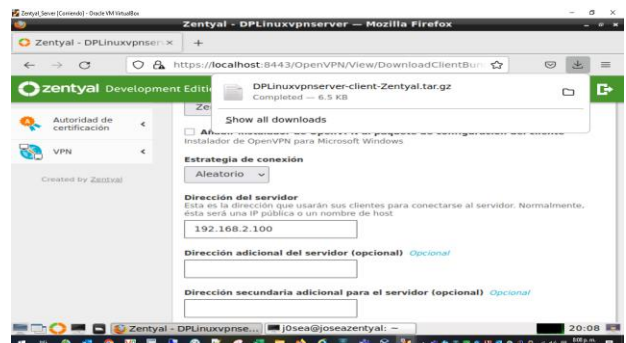


Imagen 41 Descarga exitosa de archivo para cliente vpn

Si se desea optar por implementar la conexión en equipo cliente con la herramienta openvpn, se realiza la instalación de openvpn para acceder al servidor. Después de la instalación se valida que el servicio esté corriendo: sudo service openvpn status, sino está corriendo se puede iniciar con el comando: sudo service openvpn start

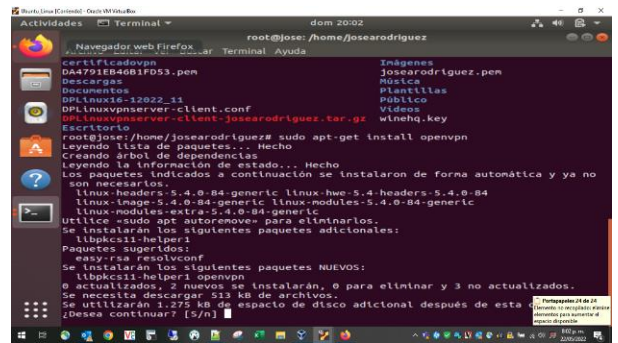


Imagen 42 Comando sudo apt-get install openvpn

Al realizar el reinicio del sistema operativo, podemos realizar la configuración, importando el archivo de configuración de vpn cliente, en la opción de configurar red cableada. En la opción de VPN, se da clic en el signo +, y se importa el archivo DPLinuxvpnsrvr-client.conf:

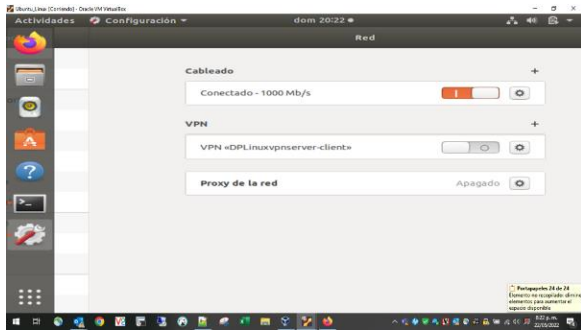


Imagen 43 Configuración VPN Cliente

Se observa que se activa un nuevo icono con la imagen de candado, dando a entender una conexión segura establecida, se valida el direccionamiento y se observa una nueva interfaz tap0 con la IP 192.168.160.2

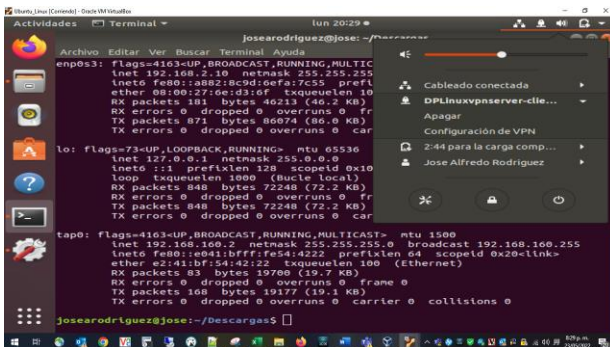


Imagen 44 Conexión VPN

Recordamos que el segmento en el servidor es 192.168.160.0/24. En la interfaz gráfica también se observa encendida la conexión de VPN:

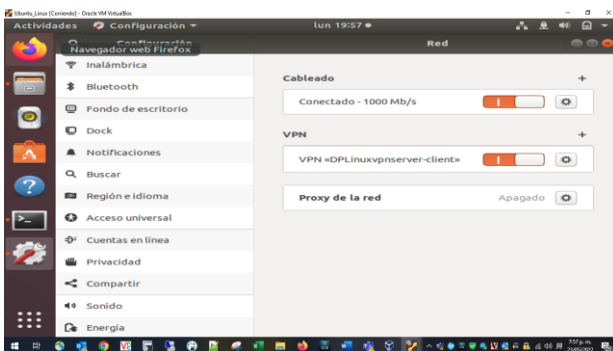


Imagen 45 Validación de conexión exitosa cliente

Si validamos al lado del servidor, también se puede visualizar la conexión del cliente desde el Dashboard

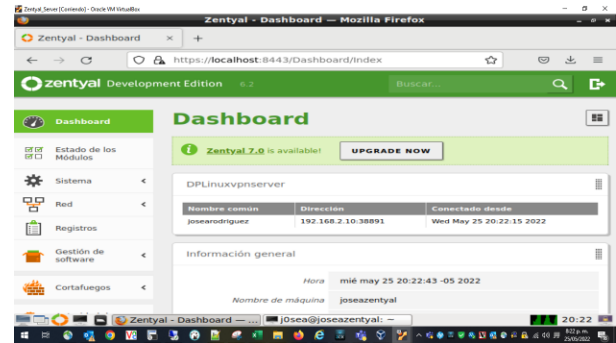


Imagen 46 Validación de conexión exitosa Zentyal Server

Finalmente, se procede a realizar pruebas de conectividad y n pruebas de navegación desde el equipo cliente de manera exitosa:

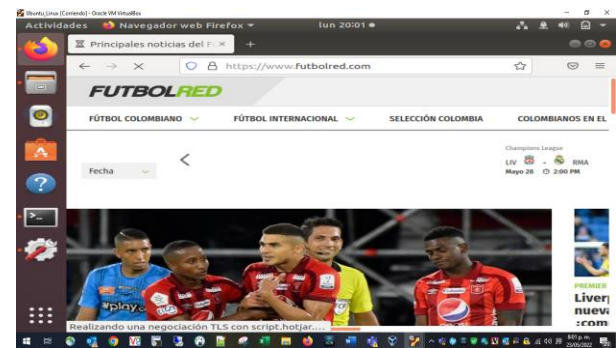


Imagen 47 Validación de navegación equipo cliente

4 CONCLUSIONES

En el mercado debemos aprender a buscar alternativas a lo convencional ya que como sabemos el sistema operativo Windows server es demasiado costoso por lo que todas las empresas no van a poder pagarlo. Nosotros como encargados de la infraestructura tecnológica de una compañía debemos hacer una búsqueda de las herramientas que estén acorde al presupuesto que se tenga y que nos ayuden a cumplir con todas los procesos y procedimientos internos (Henry Andres Fraile Gonzalez).

La utilización del servicio de Proxy No transparente nos permitió controlar de una manera segura y adecuada el acceso a internet del equipo cliente, mediante la configuración y establecimiento de reglas de acceso, que posibilitaron la solución a esta necesidad específica del cliente. (Andrés Londoño)

Se conocen las ventajas de denegar el acceso a una red social a través del servicio de firewall de Zentyal server, teniendo en cuenta que por medio del servicio de red de este servidor se pueden crear objetos, los cuales contienen miembros, con rangos de ip. (Edward Rincón)

A través del desarrollo de la presente actividad fue posible conocer y aprender sobre el sistema operativo GNU/Linux Zentyal Server, al igual que su instalación y

configuración para disponer de los servicios de Infraestructura IT, conocer las principales características que nos ofrece esta herramienta para cada uno de los servicios, especialmente para los servicios de File Server y Print Server, los cuales trabajen en la temática elegida. (Maryuri Ramirez)

Se carga el módulo de autoridad de certificados y módulo de VPN de manera exitosa, se realiza la configuración de servidor VPN, ajustando perfil, puertos, direccionamiento y tiempo de expiración. Adicional, se logra descargar el paquete de configuración de vpn cliente para un sistema operativo Linux, se copia al equipo cliente mediante una conexión ssh. Logrando configurar y establecer conexión vpn de manera exitosa. (Jose Rodriguez)

5 REFERENCIAS BIBLIOGRÁFICAS

[1] Canonical (2020). cuentas de usuario Ubuntu 18.04 LTS. Help Ubuntu. [En línea]. Disponible en: <https://help.ubuntu.com/stable/ubuntu-help/user-accounts.html.es>

[2] Gómez, L. J., & Gómez, L. O. D. (2014). Administración de sistema operativos. [En línea]. Disponible en: <https://elibronet.bibliotecavirtual.unad.edu.co/es/ereader/unad/62479?page=219>

[3] Zentyal 6.2 Documentación Oficial — Documentación de Zentyal 6.2. (s/f). Zentyal.org. Recuperado el 22 de mayo de 2022, de <https://doc.zentyal.org/6.2/es/>

[4] ProngeRTV. Como instalar y configurar un servidor VPN en Zentyal – Tutorial 2000 <https://youtu.be/8zaxU1C7qBc>

[5] Mullvad VPN. OpenVPN installation on GNU - Linux . https://mullvad.net/en/help/linux-openvpn-installation/?gclid=Cj0KCQjwvqeUBhCBARIsAOdt45ZvzOFIR9791ZT2j2gHZH3bYHsL5aNUc8sfYdzeuvlUKkZyxrws7xEaAIRnEALw_wcB