SERVICIOS QUE FORTALECEN LAS TI CON LA CONFIGURACIÓN ZENTYAL

Sara Mejia Zabala
e-mail: semejiaz@unadvirtual.edu.co
Ivone Andrea Dorado Ovalle
e-mail: iadoradoo@unadvirtual.edu.co
Jhoan sebastian Angarita Rojas
e-mail: jsangaritar@unadvirtual.edu.co
Humberto Enrique Sosa Cadena
e-mail: hesosac@unadvirtual.edu.co
Johan Manuel Borges Londiol
e-mail: jmborgesl@unadvirtual.edu.co

RESUMEN: *El siguiente documento contiene funcionalidades del Zentyal, permitiendo reconocer de forma clara el funcionamiento para aplicar las diferentes configuraciones que establezcan conectividad para brindar seguridad y de igual forma diferentes servicios requeridos ya que este permite establecer procesos para satisfacer necesidades personales o empresariales.*

PALABRAS CLAVE: Proxy no transparente, VPN, DHCP, File server

1 INTRODUCCIÓN

Zentyal es un distribuidor Linux que se puede ser insertado en cualquier entorno Windows, inicialmente es un servidor que se implementa para que este sea convertido en una alternativa de servidor para diversas empresas y organizaciones de diferente partes del mundo.

Zentyal entre sus características permite una administración de usuarios, grupos de seguridad, de listas de distribución y contactos por medio de árboles. Se puede decir que es compatible con Windows y contiene toda la configuración de ACL para usuarios y grupos. Cuenta con protocolos de correo compatibles, sincronizaciones de dispositivos móviles, diferentes dominios de correos virtuales y autenticaciones de sesión única, todo el tema de configuraciones de red, enrutamiento, DHCP server, DNS, Proxy no transparente, cortafuegos, file server y print server, VPN.

Es posible configurarlo de manera fácil y sencilla por su entorno gráfico presentado en su aplicación web.

2 CONFIGURACIÓN INICIAL

2.1 REQUERIMIENTOS

En todos los procesos de instalación y configuración se debe tener en cuenta la arquitectura del S.O, teniendo en cuenta esto, los requerimientos mínimos para su instalación son los siguientes:

CPU de 64 bits
1GB de RAM
80 GB de disco (HDD, SSD)

Realizamos la descarga de Zentyal 6.2 en el siguiente enlace: http://download.zentyal.com/zentyal-6.2-development- amd64.iso

Agregamos el archivo ISP al VirtualBox y realizamos las configuraciones necesarias para cargar el sistema.

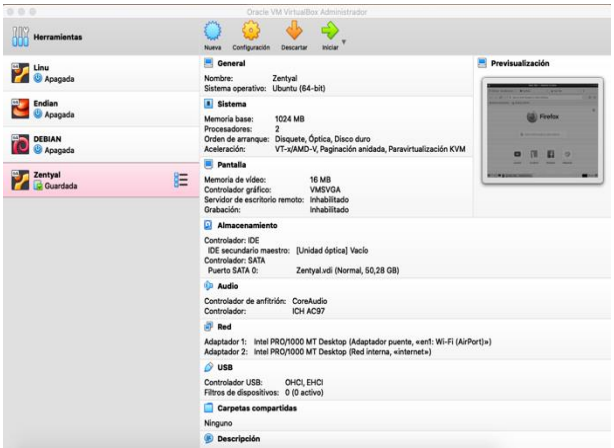


Figura 1. Cargue del archivo ISO

Iniciamos la instalación y seleccionamos el idioma de preferencia.

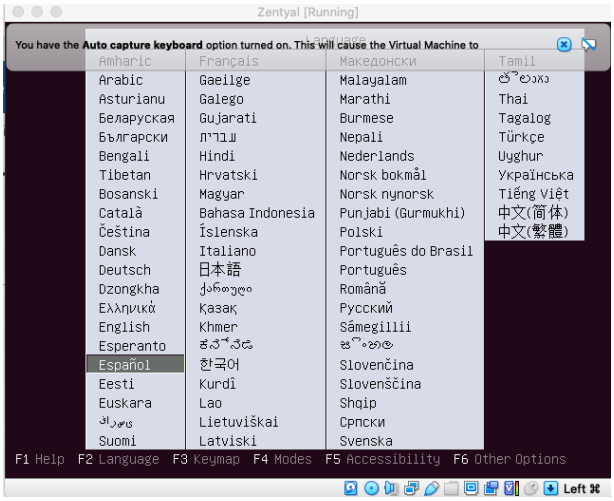


Figura 2. Selección de idioma

Seleccionamos la opción de borrar todo el disco para que se haga efectiva la instalación.

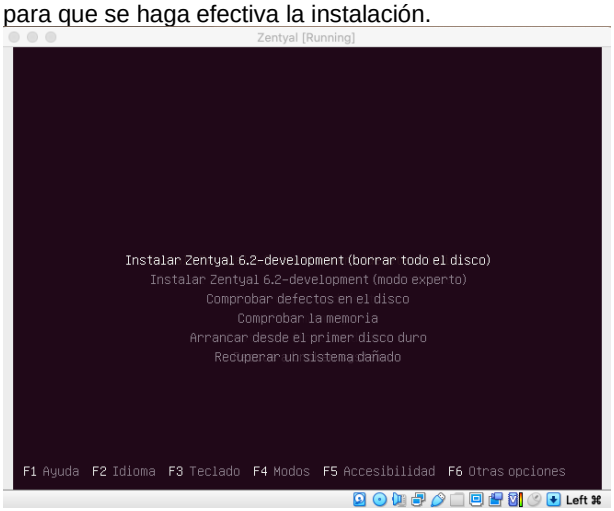


Figura 3. Selección borrada de disco.

Seleccionamos nuestra ubicación.

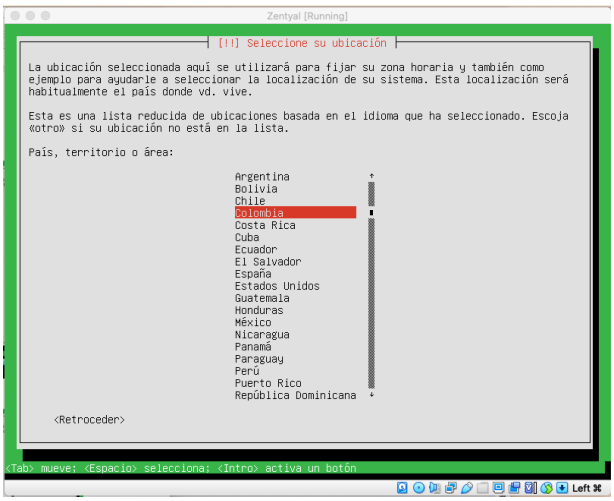


Figura 4. Selección de ubicación.

Configuramos nuestro teclado con el idioma de preferencia.

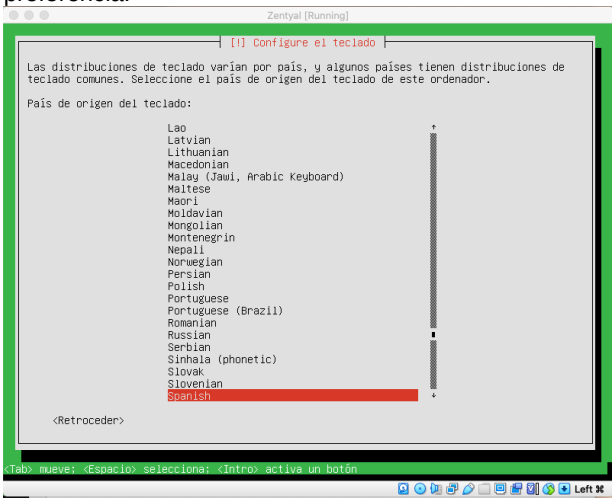


Figura 5. Selección de idioma de teclado

Realiza instalaciones y nos indica que ingresemos el nombre de la máquina.

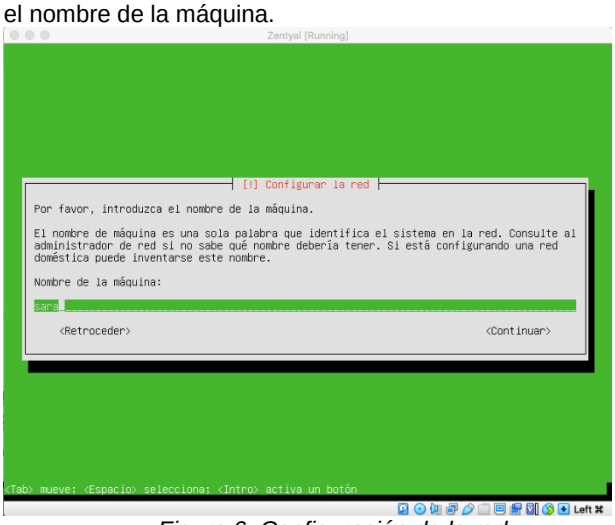


Figura 6. Configuración de la red.

Nos pide nombre de usuario y contraseña.

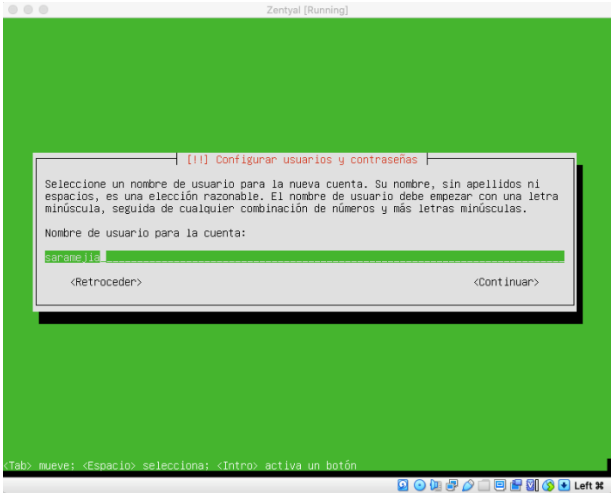


Figura 7. Nombre de usuario

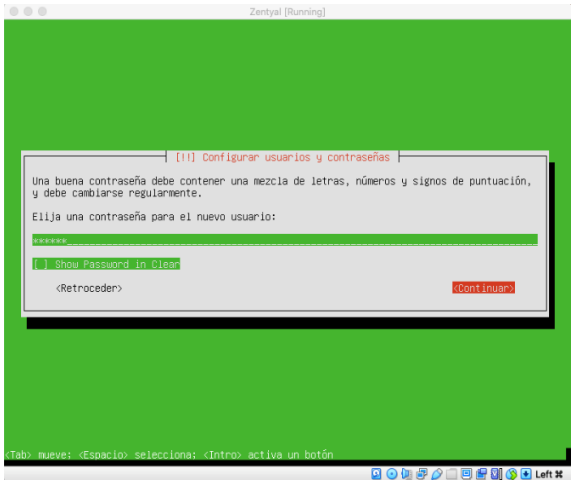


Figura 8. Contraseña del usuario.

Para finalizar, nos muestra la interfaz gráfica de Zentyal

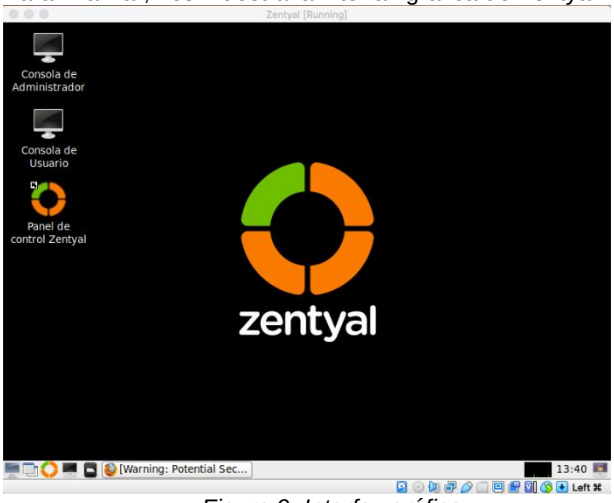


Figura 9. Interfaz gráfica.

Abrimos el panel de control de Zentyal, ingresamos con nuestro usuario y contraseña ya creados y vamos a configurarlo.

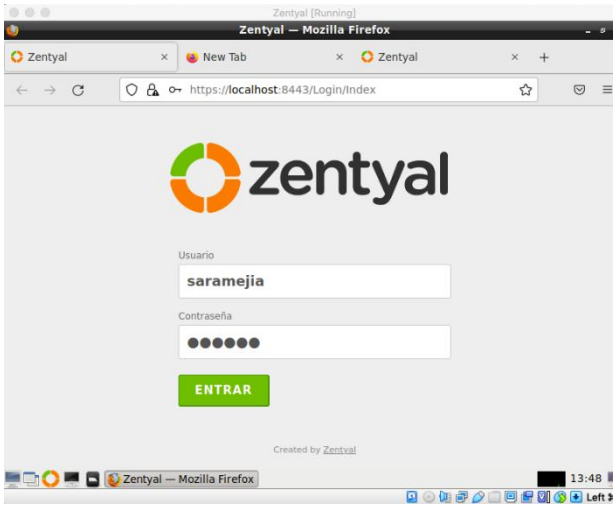


Figura 10. Ingreso a Zentyal.

Luego de haber ingresado, vamos a seleccionar los paquetes necesarios para aplicar las diferentes configuraciones.

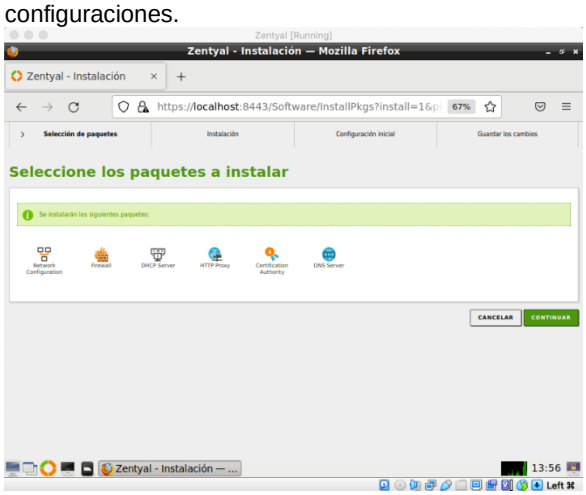


Figura 11. Paquetes a instalar.

Realizamos la configuración de las interfaces, es importante ya que gracias a estas podremos tener una buena conectividad. Es recomendable tener una interna y externa donde tendremos acceso a internet y a la infraestructura que se va a realizar.

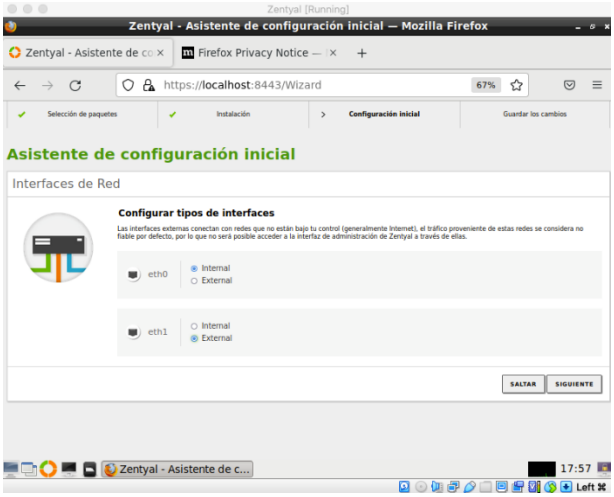


Figura 12. Configuración de tarjetas.

Luego de haber configurado esto ya nos va a permitir ingresar y empezar a desarrollar cada uno de los puntos solicitados.

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

Al instalar Zentyal se abre de manera automática el Dashboard y procedemos a seleccionar los servicios a instalar.

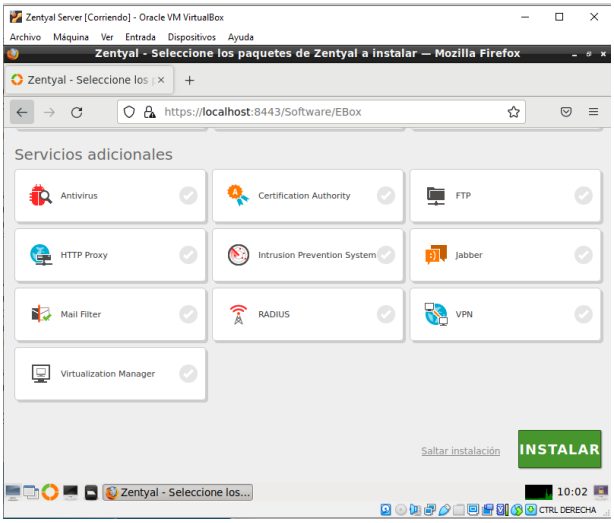


Figura 13. Selección de servicios.

Servicios seleccionados:

Domain Controller and File Sharing
DNS Sever
DHCP Server
Firewall

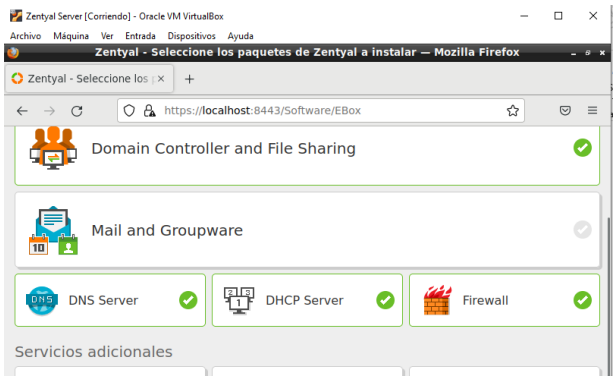


Figura 14. Selección de servicios.

Instalación de paquetes

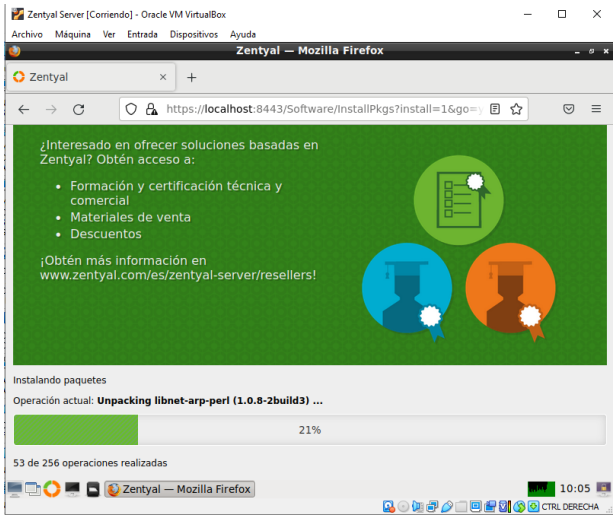


Figura 15. Instalación completa

Ingreso a Zentyal con el usuario y contraseña creado en la instalación de Zentyal.

Figura 16. Ingreso a Zentyal.

Iniciamos con la configuración del Dashboard

DHCP SERVER, DNS SERVER Y CONTROLADOR DE DOMINIO

Procedemos con la configuración de interfaz de red.

Configuración interfaz de red **eth0**
Red interna
Ip:10.0.2.15
Nombre: etho
Metodo: DHCP

Figura 17. Interfaz de red eth0

Configuración interfaz de red **eth1**

Nombre: eth1
Metodo: Estatico
Ip: 192.168.1.15
Mascara de red: 255.255.255.0

Figura 18. Interfaz de red eth1

Figura 19. Configuración puerta de enlace

Configuración del dominio

Función del servidor: Controlador de dominio
Nombre del dominio: Domain
Descripción del servidor: Zentyal Server
Letra de unidad: H

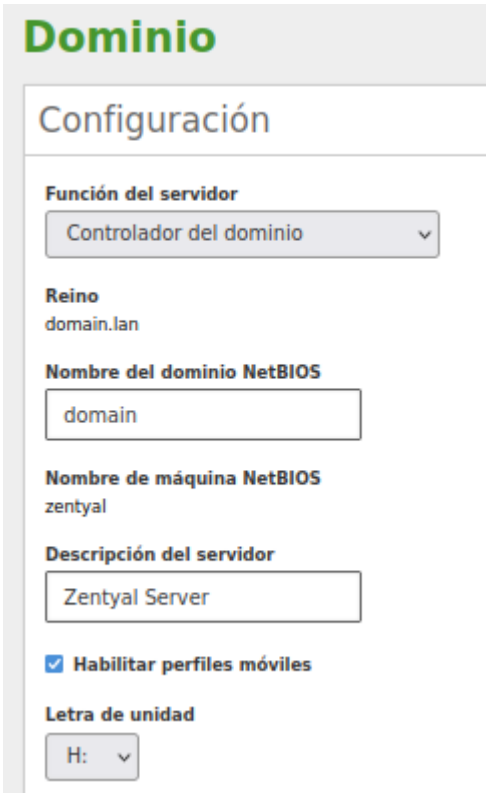


Figura 20. Configuración del dominio

Configuración del DNS
Añadimos el dominio creado DOMAIN.LAM

Configuración puerta de enlace Red **eth0**
Puerto del proxy: 8080

Figura 21. Configuración DNS

Configuración Del DCHP

Se enlaza a la Interfaz: eth1

Figura 22. Configuración DHCP

Opciones personalizadas.

Figura 23. Configuración DHCP

Asignación del rango DCHP

Dirección ip de interfaz: 192.168.1.15
Subred: 192.168.1.0/24
Asignación del rango: 192.168.1.25 a 192.168.1.35

Figura 24. Configuración DHCP

Rangos

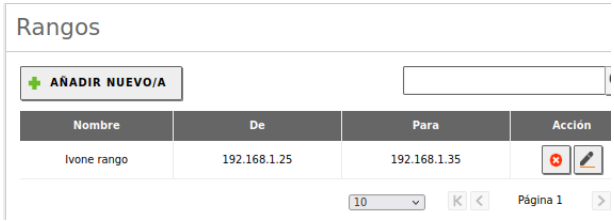


Figura 25. Configuración DHCP

Opciones del DNS

Asignamos el dominio asignado en los pasos anteriores Domain.lan

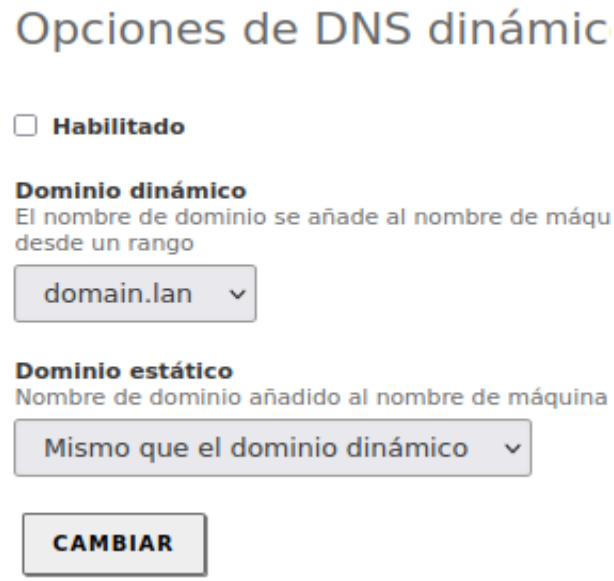


Figura 26. Configuración DHCP

Implementación y configuración detallada del acceso de una estación de trabajo GNU/Linux a través de un usuario y contraseña

Creación del usuario en Zentyal

Usuarios y equipos
users -Domain admins ivoneovalle
Usuario*: Ivonedorado.*

Figura 27. Creación de usuarios

Se realizará enrolamiento desde el sistema operativo Linux mint hacia zentyal con el comando

sudo apt-get -y install realmd sssd sssd-tools samba-common krb5-user packagekit samba-common-bin samba-libs adcli ntp

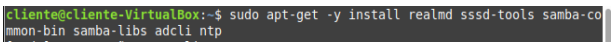


Figura 28. Ejecución de enrolamiento.

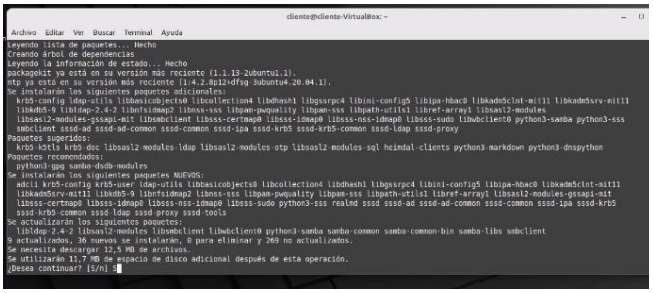
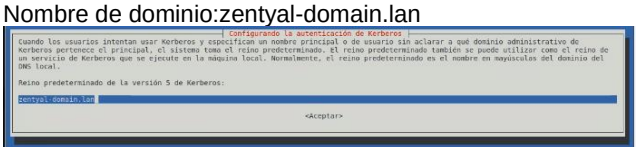


Figura 29. Ejecución de enrolamiento exitosa

Nombre de dominio:zentyal-domain.lan



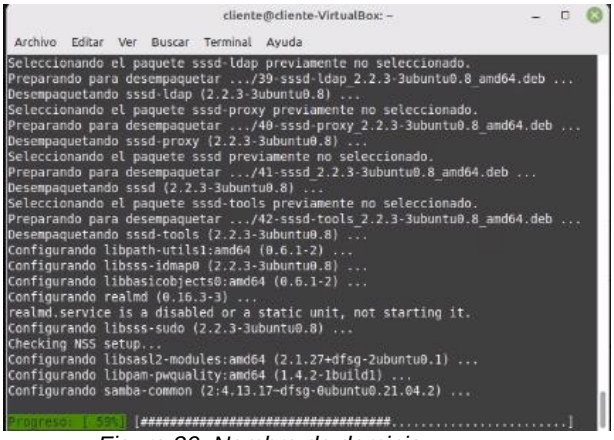


Figura 30. Nombre de dominio.

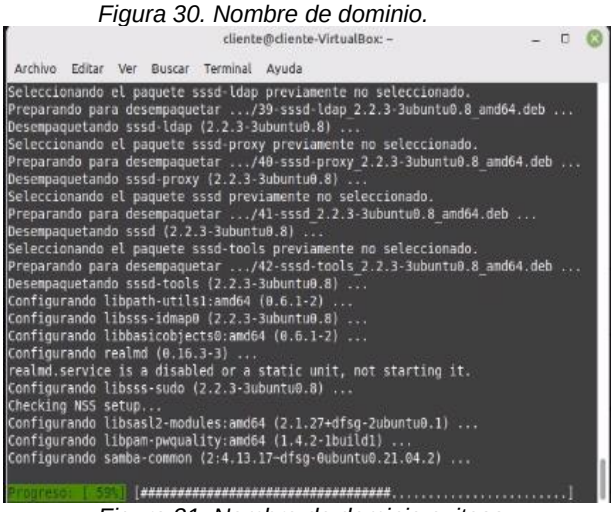


Figura 31. Nombre de dominio exitosa.

Respuesta exitosa de enrolamiento

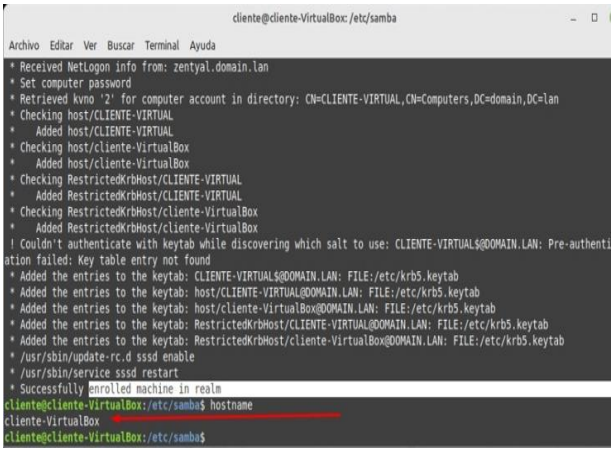


Figura 32. Enrolamiento de maquina cliente.

Se ve reflejado el dominio creado DOMAIN.LAN registro de dicha estación en los servicios de Infraestructura IT de Zentyal

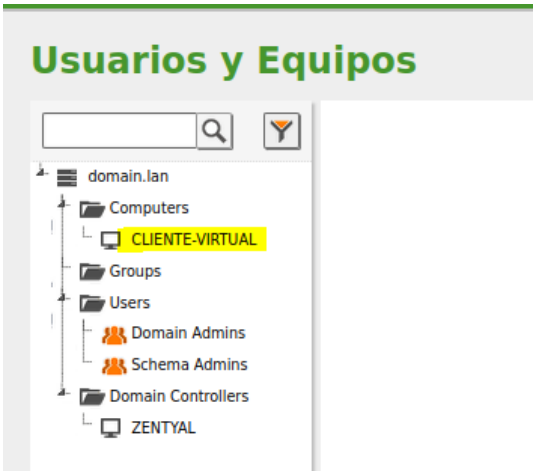


Figura 33. Enrolamiento de maquina cliente. visible

4 TEMÁTICA 2: PROXY NO TRANSPARENTE.

Para el desarrollo de este punto, es necesario instalar los siguientes componentes para realizar las respectivas restricciones del proxy.

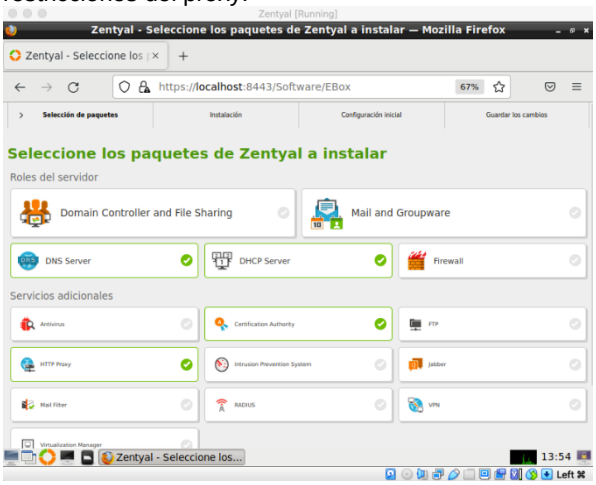


Figura 34. Componentes para el proxy no trasnparente.

Continuamos con la configuración y por medio de la consola verificamos la IR de red asignada.

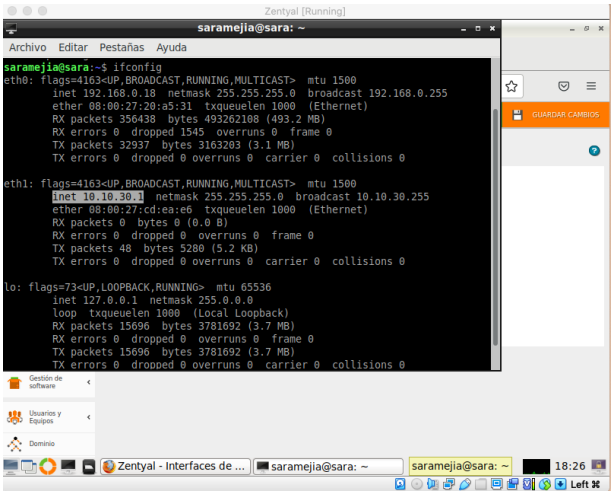


Figura 35. IP de Zentyal

Hacemos asignacion de rangos de direcciones IP para que el Ubuntu se pueda conectar por cualquiera de estos.

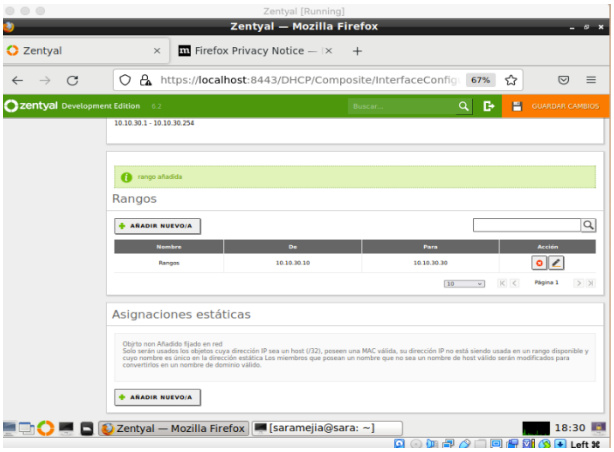


Figura 36. Rangos de dirreciones IP permitidos.

Creamos un objeto con los datos de la máquina del cliente ya que se necesta autorizar al Ubuntu.

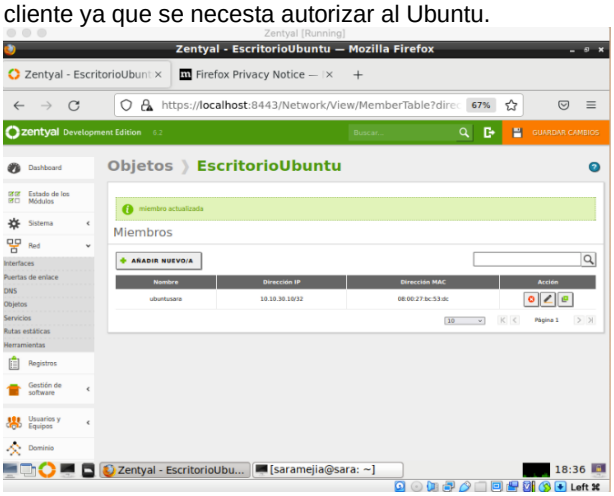


Figura 37. Creacion de un objeto

Se empieza a implementar el filtrado a traves del proxy HTTP por el puerto 1320, teniendo en cuenta que es un proxy no trasparente hacemos la configuracion de forma manual en la maquina del cliente para que tome las restricciones otorgadas.

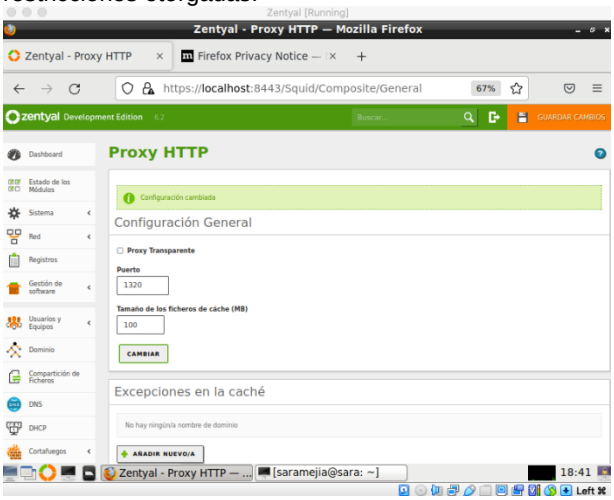


Figura 38. Apertura del puerto 1320

Continuamos con la creación de un perfil llamado bloqueos para restringir las páginas no autorizadas a través del proxy.

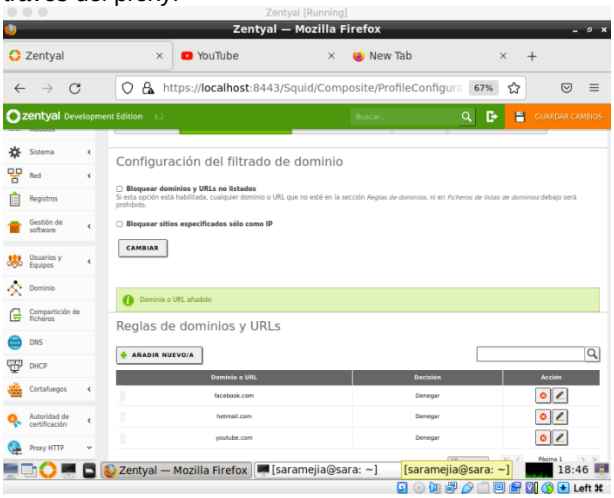


Figura 39. Creacion de perfil.

Configuramos las reglas de acceso permitiendo enlazar las restricciones al cliente y con cual perfil quedaran las restricciones de la maquina Ubuntu. También podríamos poner el filtrado por horarios y días específicos.

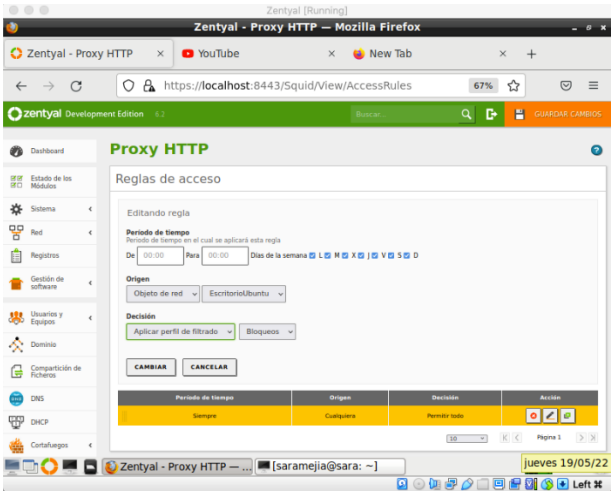


Figura 40. Implementación de reglas de acceso.

Ingresamos desde el cliente para probar la navegación a una de las páginas restringidas, podemos ver que navega normalmente.

Figura 41. Ingreso a facebbok.com

Realizamos la configuración manual desde el navegador de Ubuntu donde ingresamos el número de la IP y el número del puerto establecido.

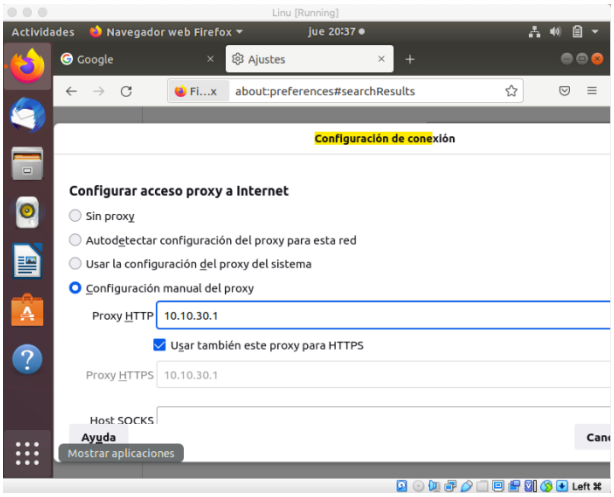


Figura 42. Configuración de conexión

Ingresamos a las páginas restringidas y verificamos que el servidor está denegando el acceso a estas páginas.

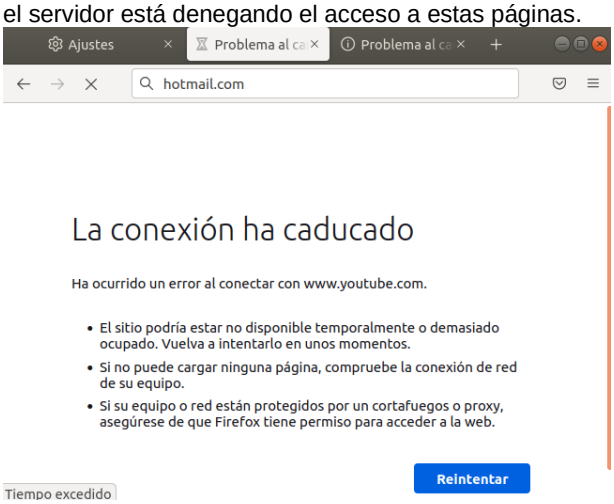


Figura 43. Acceso denegado

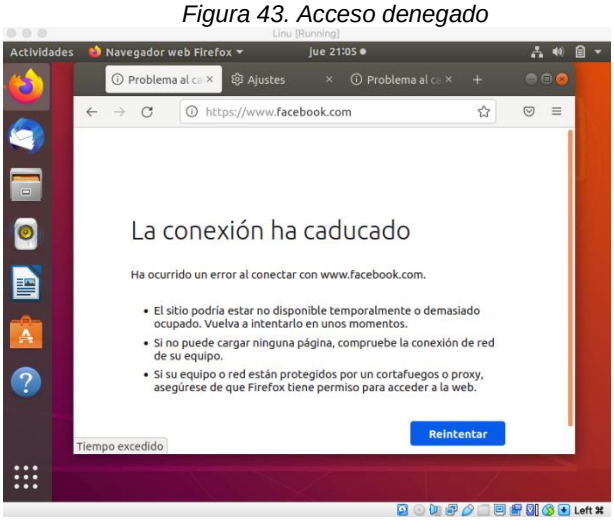


Figura 44. Acceso denegado

5 TEMÁTICA 3: CORTAFUEGOS

Los márgenes para la segunda y las páginas siguientes deben cumplir con los establecidos en el punto 2.1.

Para realizar la configuración del cortafuegos debemos primero instalar los módulos firewall y DNS server para poder acceder a las opciones de cada uno.

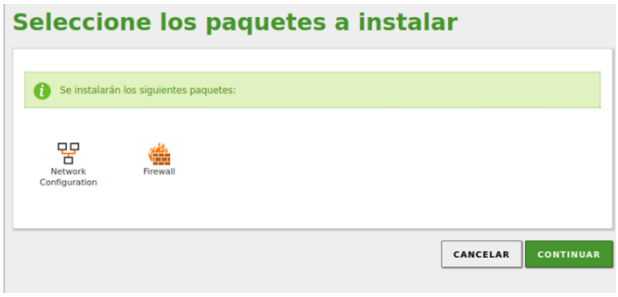


Figura 45. Instalación de módulos Firewall y red

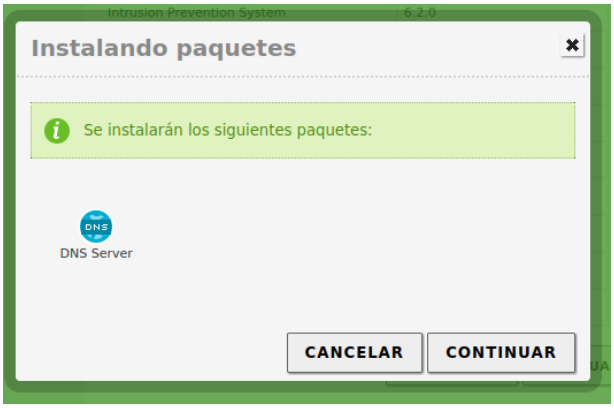


Figura 46. Instalación de módulos DNS server

Vamos a crear una máquina virtual que funcionará como equipo desktop dentro de la red interna para verificar el funcionamiento del firewall

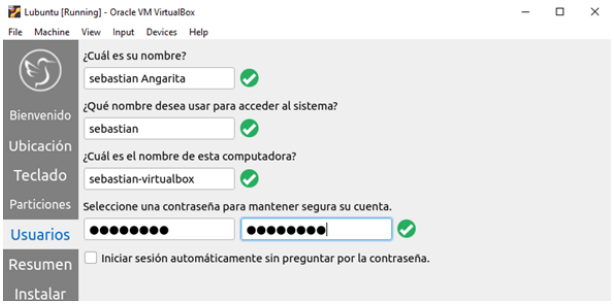


Figura 47. Instalación y configuración de Lubuntu

Ahora podemos configurar nuestro Zentyal para bloquear los siguiente sitios web que serán usados para la prueba de este ejercicio:

- Facebook
- Instagram
- Youtube
- Netflix

En el apartado de redes vamos a la opción objetos y vamos a crear uno por cada sitio web que vamos a bloquear

Figura 48. Creación de objetos por cada sitio web

Con los objetos creados podemos apreciar que podemos asignarles un miembro a cada uno, estos miembros corresponderá a las ip de cada dominio.

La forma más práctica de hallar las direcciones ip de estos sitios es con el comando “ping” y el nombre del dominio.

Figura 49. uso del comando ping a dominios

Con la dirección obtenida del comando ping ya podemos crear el miembro el cual servirá como referencia para la dirección ip que queremos bloquear. Para diligenciar este miembro solo tenemos que asignarle un nombre e ingresar la dirección ip correspondiente.

Figura 50. creación de miembro para el objeto

Con el objeto creado ya podemos asignarlo a una regla para bloquear su acceso. Para realizar esto nos dirigimos al apartado de firewall y entramos a la opción de reglas de filtrado para las redes internas.

Figura 51. Panel de reglas de filtrado para las redes internas

Ingresados en este panel vamos a crear una nueva regla, esta regla tiene que ser del tipo denegar y va a evitar la conexión desde cualquier origen *(representando cualquier usuario en la red interna).* al destino que será nuestro objeto *(el cual representa las direcciones ip del sitio web a bloquear)*

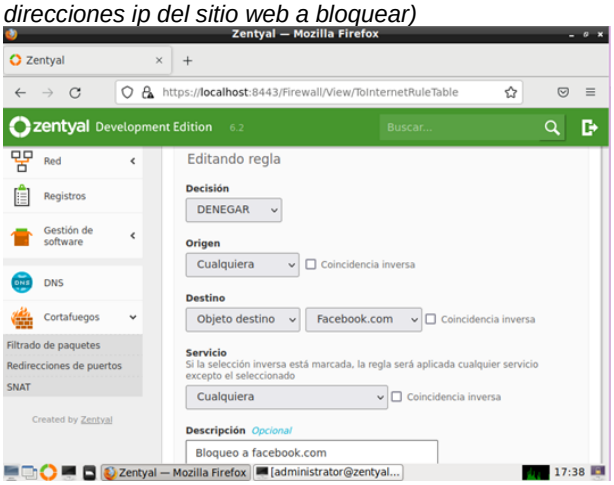


Figura 52. Creación de reglas para redes internas

Antes de guardar los cambios y reiniciar la red vamos a verificar que en nuestro equipo escritorio se encuentre conectado a internet y pueda ingresar a los sitios web, en este caso probaremos primero con facebook

Figura 53. Conexión a facebook antes del firewall

Ahora guardaremos los cambios y esperamos a que Zentyal restablezca la conexión, cuando nuevamente

tengamos conexión a la red interna verificamos nuevamente si podemos ingresar al dominio de Facebook,

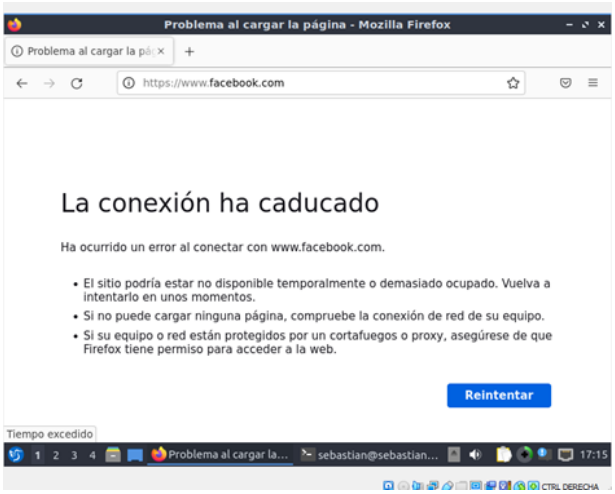


Figura 54. Conexión a facebook con firewall activado

Podemos comprobar exitosamente que el firewall se encuentra activado y configurado bloqueando la conexión de todos los equipos de la red interna a Facebook.com.

Para finalizar vamos a crear los objetos correspondientes a los demás sitios web a bloquear para generar nuevas reglas que bloqueen su acceso a la red interna

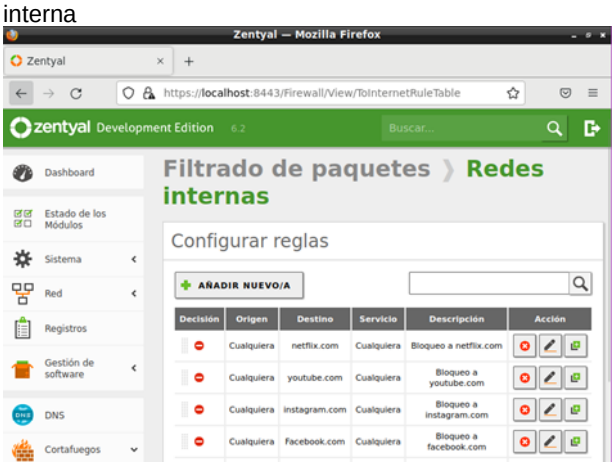


Figura 55 Reglas con los objetos de los otros sitios web

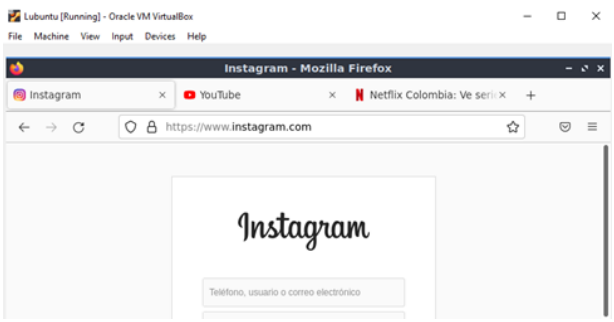


Figura 56 Sitios web antes del bloqueo

Una vez creada las reglas y asignadas a cada sitio aplicaremos los cambios y dejaremos que se reinicie la red, para poder ingresar y confirmar que no se pueda tener acceso a los sitios

Figura 57 Sitios web después del bloqueo

Como se puede apreciar en la figura # el dispositivo no pudo ingresar a los sitios web confirmando que la red interna tiene bloqueadas las direcciones ip mediante el firewall de Zentyal

6 TEMÁTICA 4: FILE SERVER Y PRINT SERVER

Seleccionamos los componentes que requerimos

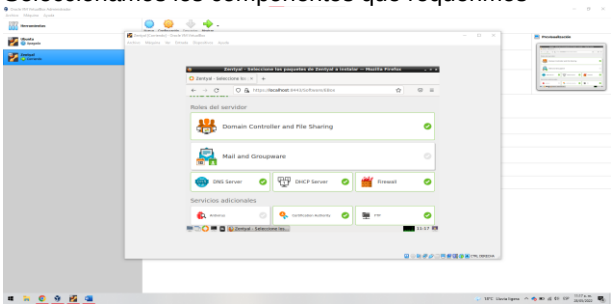


Figura 58 Componentes

Damos en el botón continuar

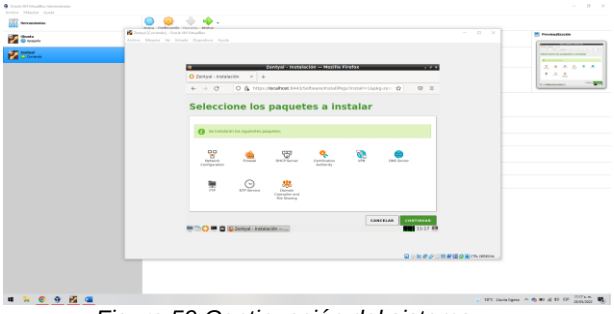


Figura 59 Continuación del sistema

Seleccionamos el tipo de interfaces

Figura 60 Interfaces

Seleccionamos el método DHCP para eth0

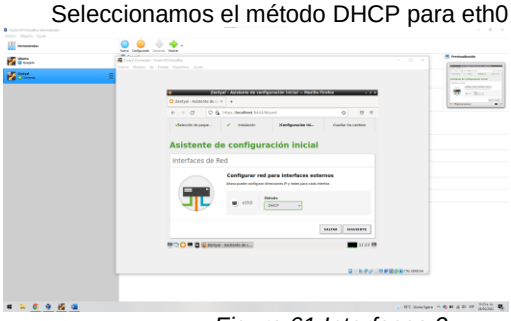


Figura 61 Interfaces 2

Ingresamos el nombre del dominio

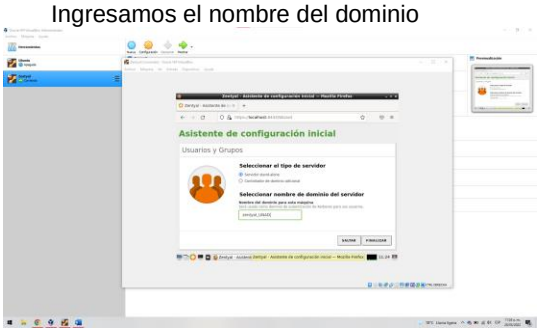


Figura 62 Nombre del dominio

El sistema muestra mensaje de bienvenida

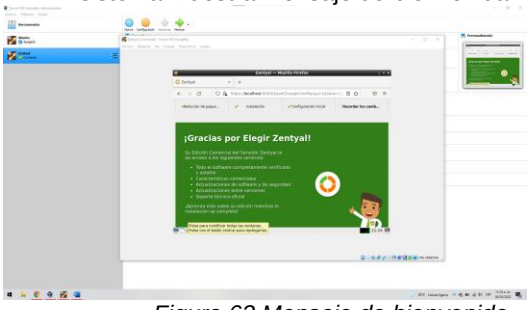


Figura 63 Mensaje de bienvenida

Seleccionamos la opción de ir al Dashboard

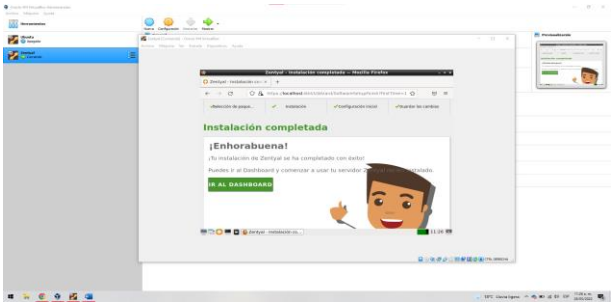


Figura 64 Ingresamos al dashboard

El sistema muestra la información básica del sistema

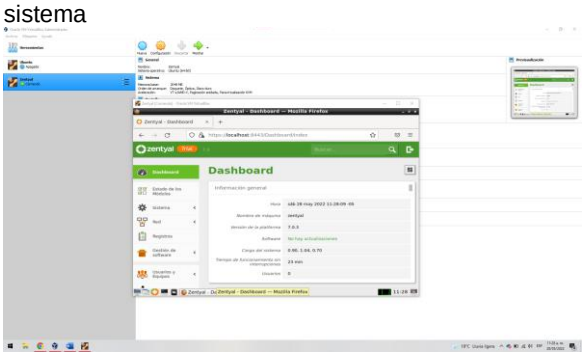


Figura 65 Información principal

Ingresamos a la configuración de DHCP

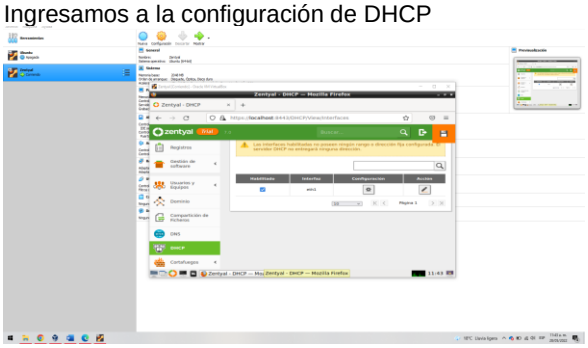


Figura 66 Configuración DHCP

Guardamos los cambios

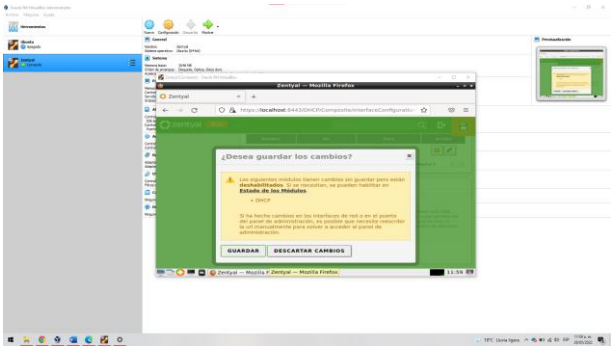


Figura 67 Guardar los cambios

Añadimos un usuario nuevo

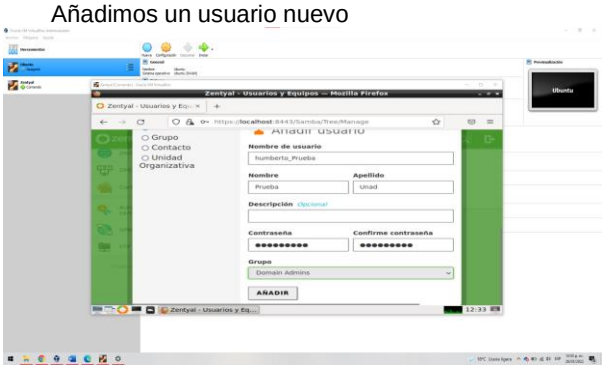


Figura 68 Usuario nuevo

Agregamos una nueva capeta comparitda

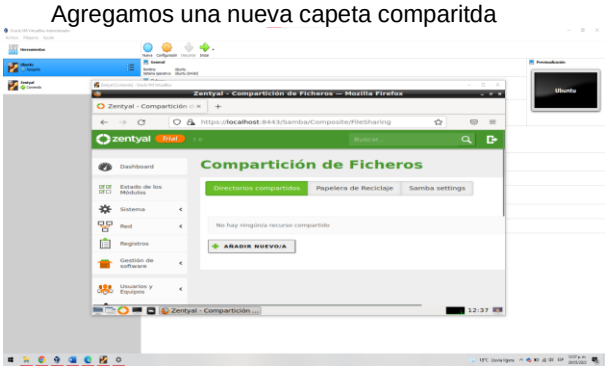


Figura 69 Fichero compartido

Información de carpeta compartida

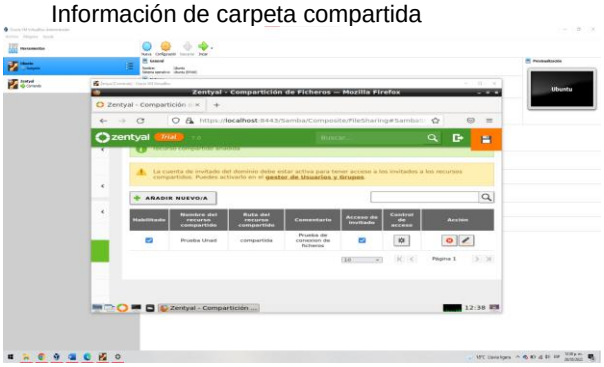


Figura 70 Información carpeta

Agregamos los usuarios que participaran en la carpeta

Figura 71 Usuarios carpeta

Guardamos los cambios

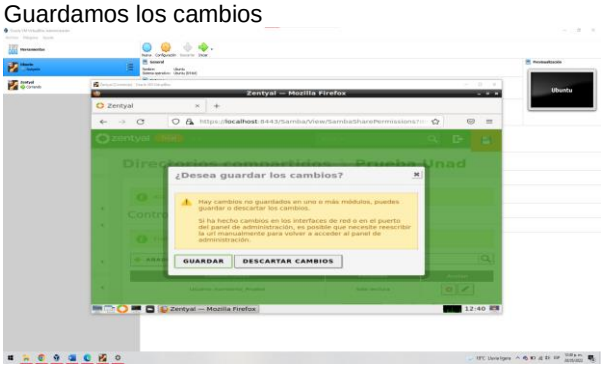


Figura 72 Guardar cambios 2

Agregamos el servidor en el archivo Resolv.conf

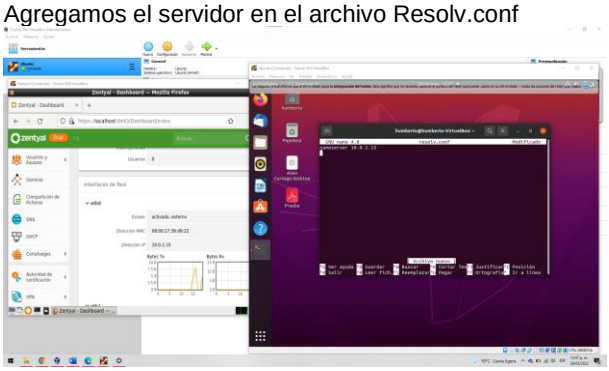


Figura 73 Archivo resolv.conf

Probamos la autenticación

Figura 74 Autenticación

7 TEMÁTICA 5: VPN

Luego de instalar el servidor de Zentyal en nuestra máquina virtual, se procede a ingresar al modulo de administracion

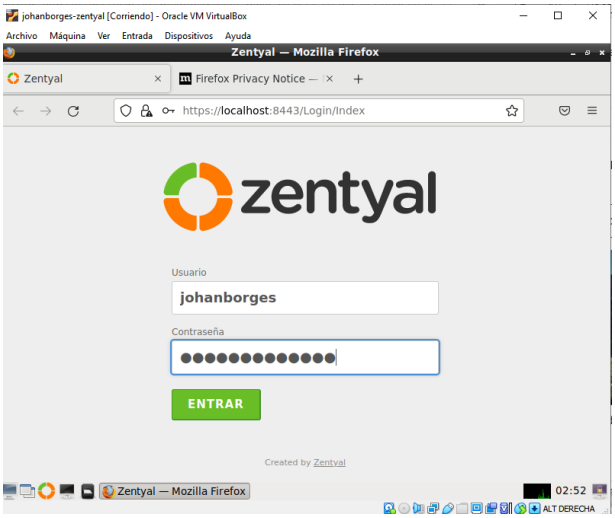


Figura 75 Autenticación

Se sigue con la instalacion del modulo de VPN:

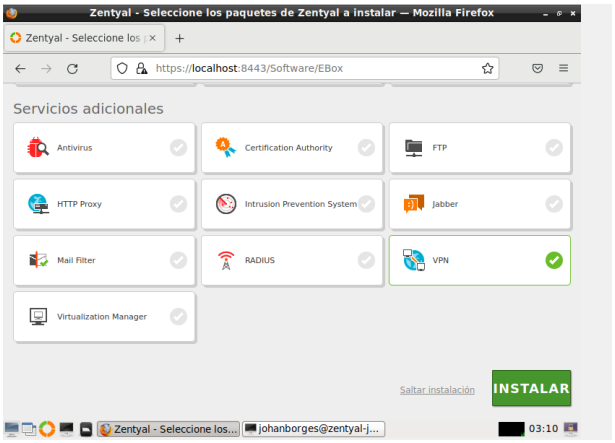


Figura 76 Servicios

En este se instalarán los paquetes de:

- Network Configuration
- Firewall
- Certification Authority
- VPN

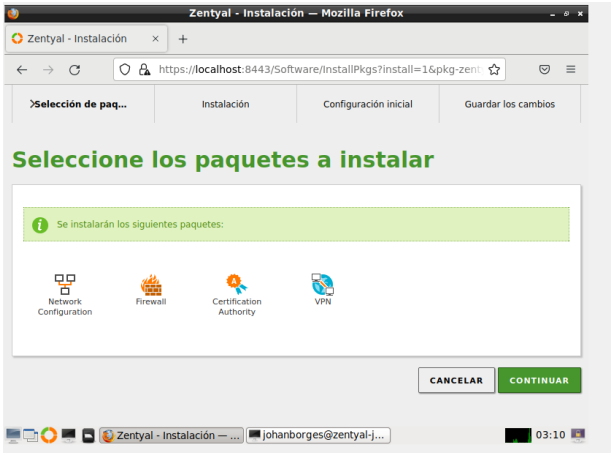


Figura 77 Paquetes

En esta parte ya inicia la instalación de los mismos

Figura 78 Paquetes

Se configuran las interfaces de red

En este caso tenemos 2

eth0: la cual se maneja como red interna (conexión clientes dentro de la misma red)

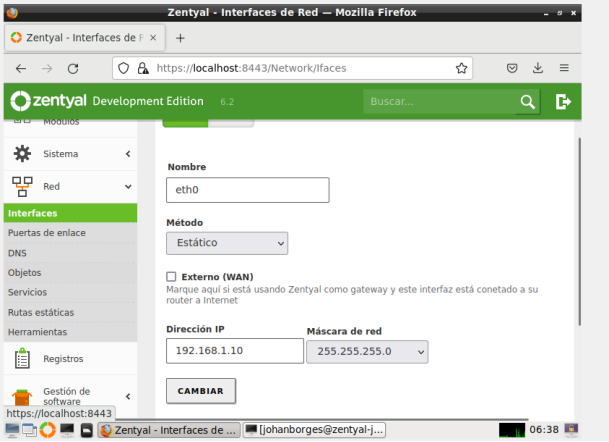


Figura 79 Interfaces

eth1:la cual se maneja como red externa(conexión a internet)

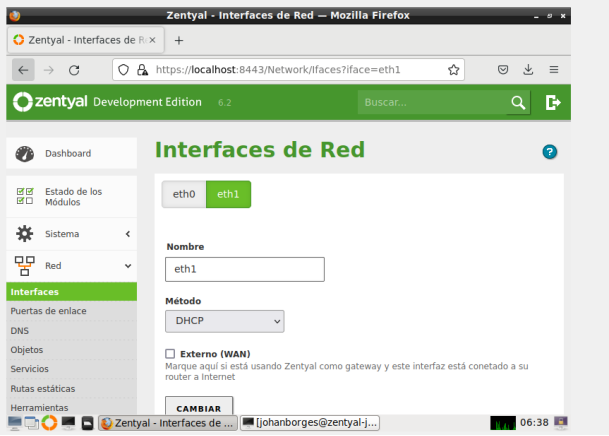


Figura 80 Interfaces

Luego se crea un Certificado de la autoridad de Certificación, con el fin de asignarlo al servidor VPN

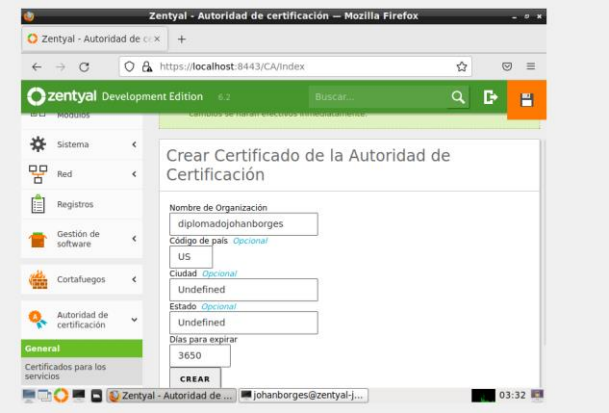


Figura 81 certificado

Evidencia del Certificado creado

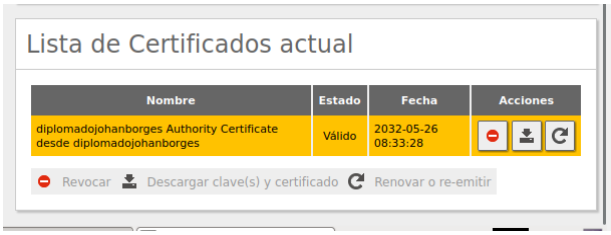


Figura 82 Certificado

Configuración de DNS para tener salida de internet y lectura de dominios en la actualización de paquetes:

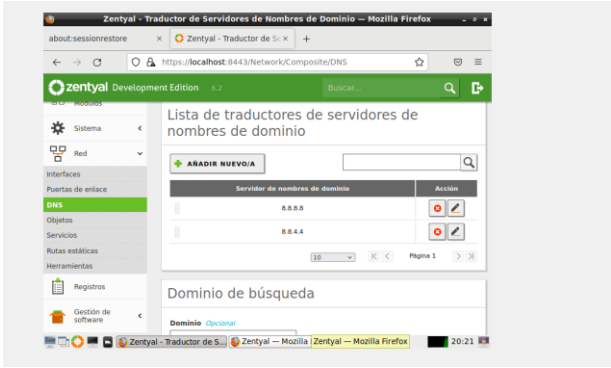


Figura 83 DNS

También se procede a configurar una puerta de enlace

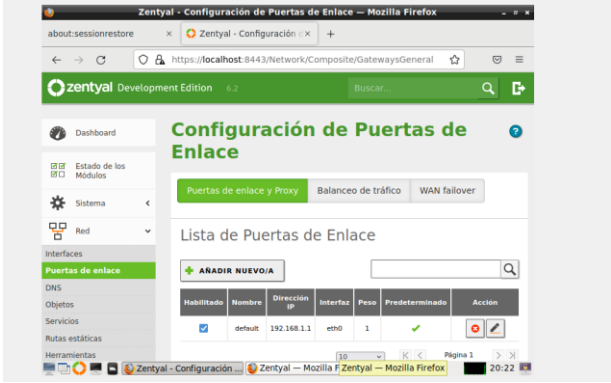


Figura 84 Puertas de enlace

En el módulo de VPN creamos el servidor dentro de la lista que nos ofrece el sistema

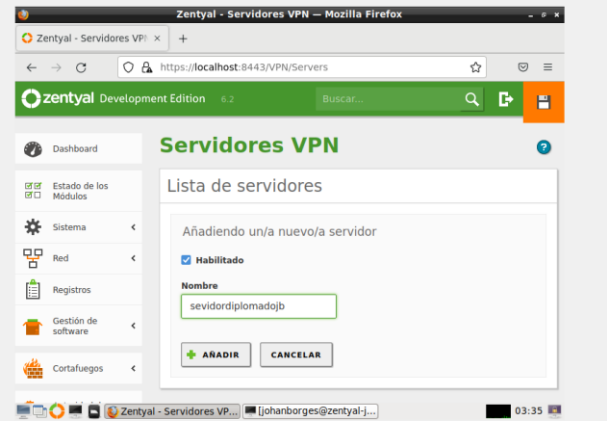


Figura 85 Servidor VPN

Se crea un nuevo certificado el cual también estará atado al servidor de VPN

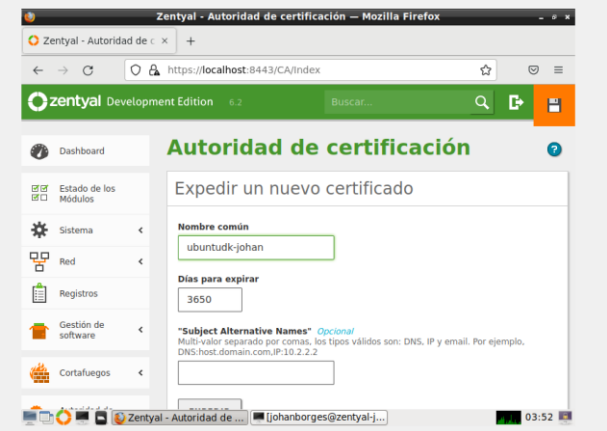


Figura 86 Certificado servidor

Ahora Dentro del apartado de configuración de nuestro servidor de VPN, asignamos el nuevo certificado

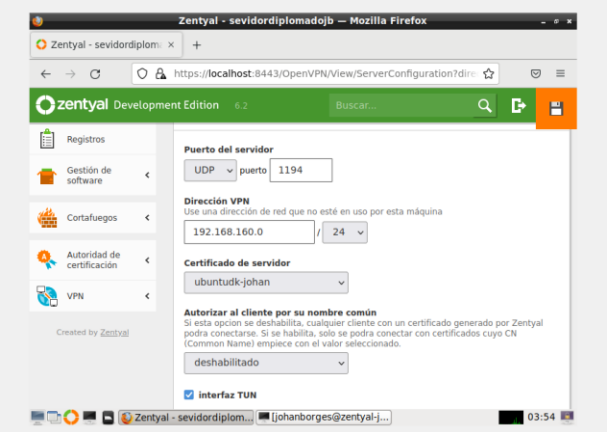


Figura 87 Certificado servidor

Ya con esto se procede a descargar el certificado de conexión para clientes linux bajo la ip del servidor (192.168.1.10)

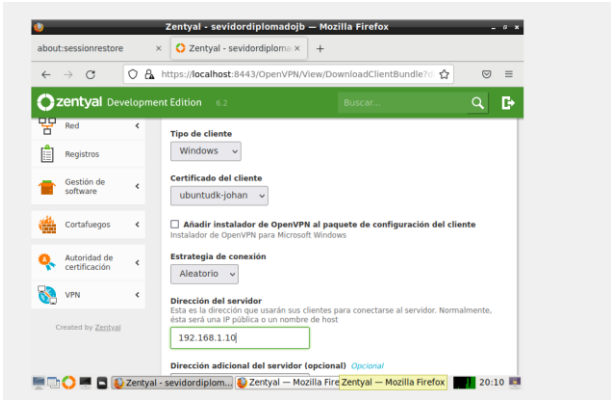


Figura 88 Certificado de conexión

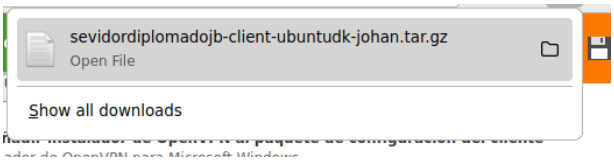


Figura 89 Certificado de conexión

Se sube el servidor de VPN y se validan los módulos activos:

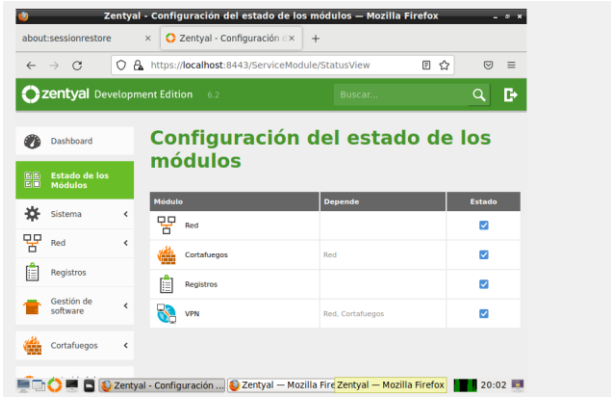


Figura 90 Estado Modulos

Ahora en el cliente UBuntu nos conectamos a través de la opción OpenVPN mediante los certificados arrojados

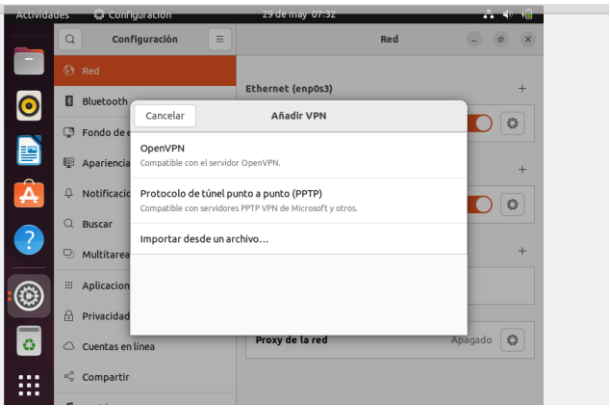


Figura 91 Conexión cliente Ubuntu

Aquí vemos los archivos .pem que cumplen de la función de certificados de conexión

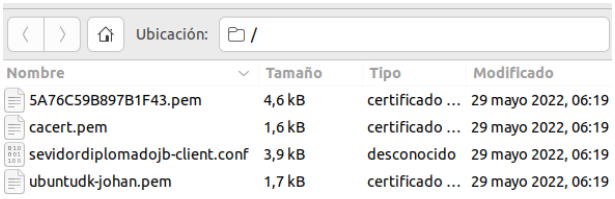


Figura 92 Archivos de Certificado

Procedemos a establecer conexión

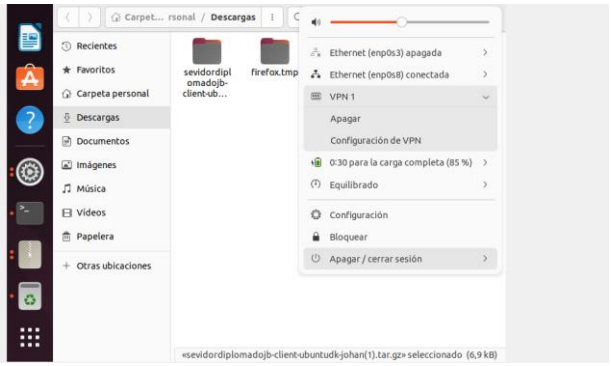


Figura 93 Conexión

8 CONCLUSIONES

· Se pudo comprender el funcionamiento del Zentyal para conectarlo con el desktop y se hizo la restricción a través del proxy 1320 para permitir el control de los usuarios conectados al servidor.

Gracias al trabajo realizado se pudo realizar la instalación y configuración de Zentyal la cual es una herramienta muy útil al momento de administrar redes internas permitiéndonos así en este caso, configurar un firewall para el bloqueo de redes sociales y sitios de entretenimiento a los usuarios de la red interna.

Zentyal es un servidor el cual cuenta con una gran cantidad de funciones útiles que se usan el día a día, nos permite crear un servidor de VPN dentro de una red interna o externa, con el fin de mejorar la seguridad dentro de los servidores que se encuentran en la misma.

Desarrollando esta actividad, logramos observar y aplicar las ventajas que tenemos con Zentyal para el manejo de archivos y carpetas compartidas por medio del File Server; las opciones que tenemos para el manejo de usuarios y los permisos que puedan tener cada uno.

9 REFERENCIAS

[1] Instalación Zentyal. (s.f.). Obtenido de https://doc.zentyal.org/6.2/es/installation.html.

[2] JGAITPRO. (s.f.). Zentyal - Instalar y configurar DHCP Server. Obtenido de https://www.youtube.com/watch?v=H5lhAKOH5LM&t=71s

[3] ZAMET. (s.f.). Parte III Configurar Zentyal DNS, Controlador de Dominio LDAP y Samba. Obtenido de https://www.youtube.com/watch?v=-cCbsg5SDns&t=1283s

[4] Zentyal 6.2 Official Documentation. (2004). Obtenido de https://doc.zentyal.org/6.2/en/

[5] Zentyal 6.2 Official VPN Documentation.. Obtenido de https://doc.zentyal.org/es/vpn.html

[6] Zentyal 6.2 Cortafuegos (2004). Obtenido de https://doc.zentyal.org/6.2/es/firewall.html