SOLUCIONANDO NECESIDADES ESPECÍFICAS EN GNU/LINUX MEDIANTE LA INSTALACIÓN Y CONFIGURACIÓN DE ZENTYAL SERVER

Diego Alexander Villalba Rozo
di88vil721@unadvirtual.edu.co
Patricia Sánchez Alonso
psancheza@unadvirtual.edu.co
Raúl Giovanni Benavides Sierra
rgbenavidess@unadvirtual.edu.co
Walter Triana Hernández
wetrianah@unadvirtual.edu.co

RESUMEN: *GNU / LINUX es un sistema operativo de licencia libre, que nace de la unión entre el sistema GNU (desarrollado por la FSF) y el núcleo o kernel Linux (desarrollado por Linus Torvalds). Desde sus inicios Linux se diseñó como un sistema multiusuario y multitarea, Linux puede ser modificado por los mismos usuarios, para ser mejorado y especializado y de esta manera atender las necesidades en los diferentes entornos y ramas de la ingeniería. En el desarrollo del curso se enfoca su manejo sobre distintas distribuciones tanto de servidores como de equipos de escritorio que ofrecen diferentes funcionalidades, servicios como: manejo de información, transferencia de datos, servicios web, seguridad informática, firewall, proxy, entre otros. Y aplicarlos a una solución de una problemática planteada como simulación a futuros retos en el desempeño profesional. Otra de las ventajas de estos sistemas de código abierto, es que su desarrollo es acompañado de documentación robusta que permite a sus usuarios entender su funcionamiento. En el desarrollo de las actividades propuestas se identificarán los servicios utilizados, las ventajas y potencial que se puede tener, al saber administrar los diferentes servicios sobre las distribuciones de Linux.*

PALABRAS CLAVE: Cortafuegos, DHCP, DNS, Proxy, Zentyal Server

1 INTRODUCCIÓN

Este documento recopila la información referente al desarrollo de la actividad final correspondiente al curso diplomado GNU/Linux denominada paso 8 solucionando necesidades específicas con GNU/Linux. Donde su tema principal es el manejo y administración del servidor Zentyal aplicando los conceptos aprendidos a lo largo del curso, poniendo en marcha el funcionamiento de diversos servicios, tanto de seguridad como de acceso a Internet a diferentes equipos clientes, los cuales serán administrados por este sistema servidor. No obstante, como primer paso realizando la instalación de Zentyal Server 6.2 en una máquina virtual y así mismo, configurar las distintas tarjetas de Red donde se implementarán dos tipos de redes del paso de WAN a una red LAN.

2 TEMÁTICA 1

2.1 DHCP Server, DNS Server y Controlador de Dominio

CONFIGURACIÓN DE ZENTYAL

Al iniciar el sistema operativo, en mi caso no cargo la tarjeta de red eth0, para activar esta interfaz de red se ejecuta el comando desde la terminal, sudo ifconfig eth0 up, este comando se ejecuta y se ejecuta sudo dhclient eth0, para que la tarjeta de red eth0 tome la red puente y así se pueda acceder a la interfaz web del servidor Zentyal, desde la siguiente URL: https://192.168.20.65:8443/.

En esta imagen se puede observar que ya se puede ingresar a Zentyal Server, en esta ocasión ingresó en modo consola.

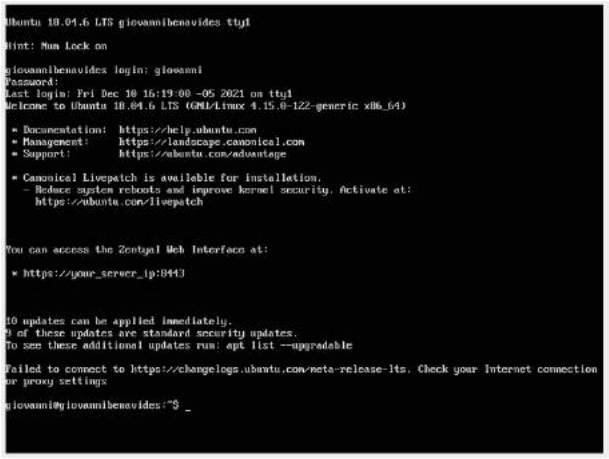

Figura 1. Ingreso al servidor Zentyal

Luego de activar la interfaz gráfica del servidor, se verifica el direccionamiento que están tomando las tarjetas de red configuradas, la tarjeta eth0 tiene la dirección 192.168.20.65. La cual es el direccionamiento de la red puente.

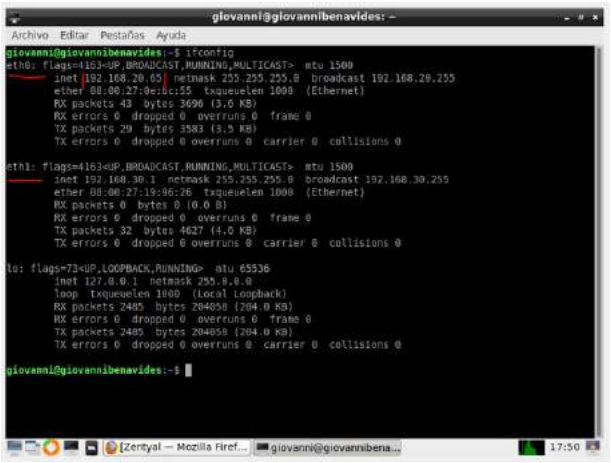

Figura 2. Verificación de tarjeta de red eth0

En esta imagen se puede observar que para esta actividad se trabaja con una máquina Desktop, que cuenta con dos tarjetas de red, un adaptador puente y una red interna.

Figura 3. Configuración de adaptador puente y red interna, en máquina Desktop

En esta imagen se puede observar que el servidor Zentyal cuenta con las dos tarjetas de red al igual que la máquina Desktop, un adaptador puente y una red interna, esta última permite la comunicación entre las dos máquinas virtuales que tomen las respectivas configuraciones.

Figura 4. Configuración de adaptador puente y red interna, en máquina Zentyal Server

En esta imagen se puede observar que se realiza un ping a la dirección 192.168.20.65, la cual es la dirección de Zentyal Server, lo cual indica que se tiene comunicación entre las dos máquinas virtuales.

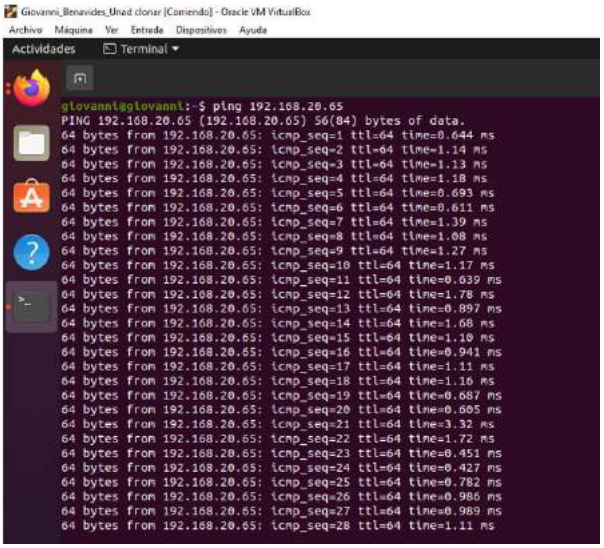

Figura 5. Ping desde la máquina Desktop, hacia la máquina server.

Se ingresa a la dirección 192.168.20.65:8443, para ingresar al entorno web de Zentyal, desde la máquina Desktop.

Figura 6. Ingreso a la interfaz web de Zentyal

En esta imagen se puede observar que ya se puede acceder a Zentyal e iniciar las configuraciones que se requieren.

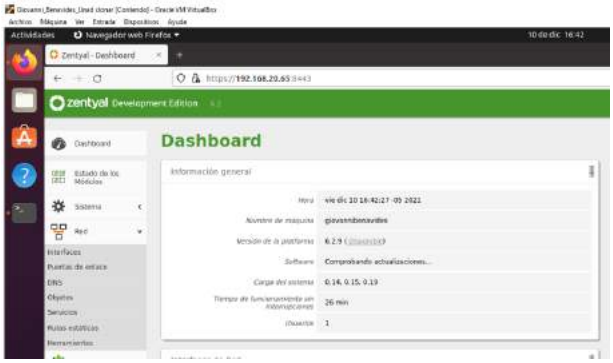

Figura 7. Ingreso a Dashboard del servidor Zentyal

CONFIGURACIÓN DHCP SERVER

Para activar el servicio de DHCP, se debe realizar la activación de estado en la configuración de los módulos, como se puede observar en la imagen.

Figura 8. Configuración del estado de módulos

En la siguiente imagen, se puede observar que ya está guardando los cambios realizados y la activación de DHCP.

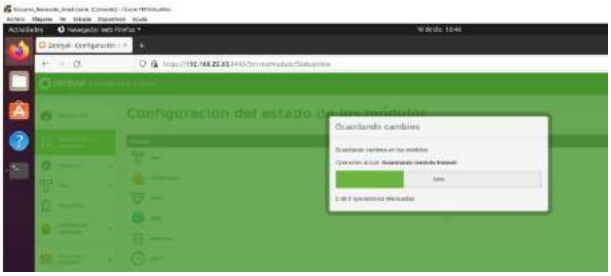

Figura 9. Guardando cambios

Luego de que el sistema termina de guardar la información, aparece un mensaje de confirmación.

Figura 10. Confirmación de configuración guardada

Antes de realizar la configuración de DHCP, se debe configurar una interfaz estática para el servidor.

Figura 11. Se requiere una interfaz estática para server DHCP

Para realizar la configuración de la interfaz, se dirige a la opción de red, selecciona la tarjeta eth1, y se agrega la dirección 192.168.30.1 y la máscara 255.255.255.255.0, como se puede observar en la imagen.

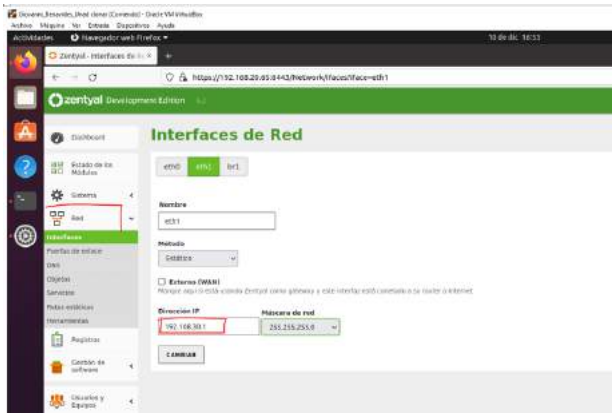

Figura 12. Configuración de interfaces de red

Luego de realizar la creación de la interfaz de red, en el módulo de DHCP, se puede observar que ya aparece y se procede a configurar el rango de direccionamiento.

Figura 13. Interfaces DHCP

Se agrega el rango DHCP y en la siguiente imagen se puede observar el rango DHCP configurado.

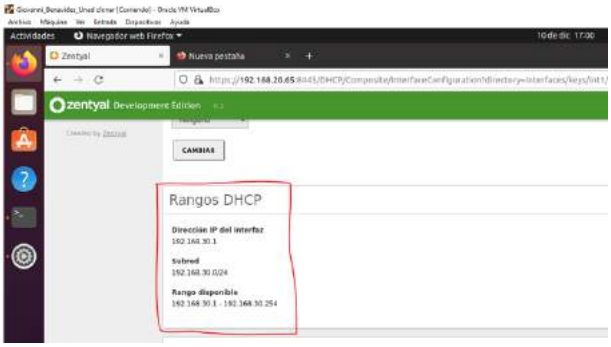

Figura 14. Rangos DHCP

En este paso se agrega el rango de direcciones que va a permitir el servidor DHCP, para esto en la opción de rangos, selecciona la opción añadir nuevo.

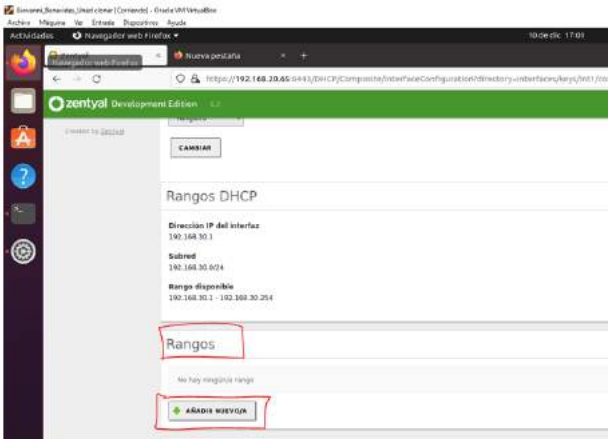

Figura 15. Configuración de rangos de direcciones DHCP

El rango que se crea de direccionamiento es el siguiente el cual va desde: 192.168.30.120 para: 192.168.30.150, para finalizar esta configuración se da clic en el botón añadir.

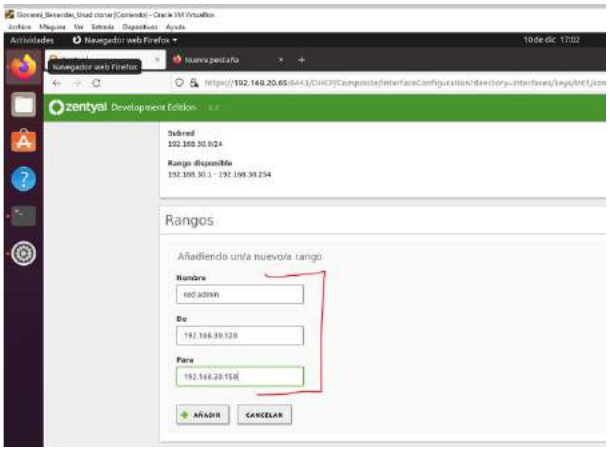

Figura 16. Añadiendo un nuevo rango de direcciones

En esta imagen se puede observar los rangos de direcciones creados anteriormente, para finalizar esta configuración, se debe guardar cambios.

Figura 17. Rangos de direcciones DHCP configurados

Luego de guardar cambios, el sistema confirma los cambios realizados.

Figura 18. Guardando cambios realizados en la creación de rangos DHCP

En esta imagen se puede observar que en el Dashboard ya aparecen varias IPs asignadas con el servidor DHCP.

Figura 19. IPs asignadas con DHCP

Para realizar esta prueba, se ejecutan varias máquinas virtuales que ya se habían trabajado anteriormente en el curso, se puede observar que ya toman el direccionamiento IP por DHCP, en este caso se observa la dirección 192.168.30.120.

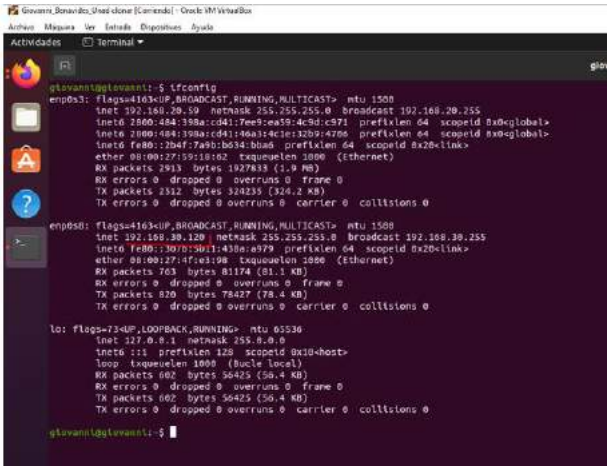

Figura 20. Verificación de direccionamiento DHCP

En esta imagen se puede observar que ya no aparece la máquina anterior ya que se apaga y se ejecuta un nuevo Desktop y esta toma direccionamiento por DHCP como se puede ver en las siguientes imágenes.

Figura 21. IPs asignadas con DHCP

En esta imagen se puede observar que la máquina virtual Desktop ya está tomando el direccionamiento configurado por DHCP y la dirección 192.168.30.122.

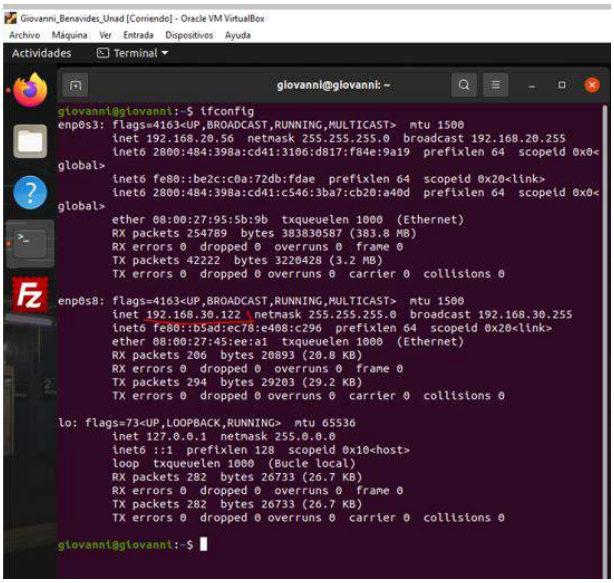

Figura 22. Direccionamiento tomado por una máquina virtual Desktop

CONFIGURACIÓN DNS SERVER

Para realizar la activación del servicio DNS, se debe seleccionar habilitar el caché de DNS transparente.

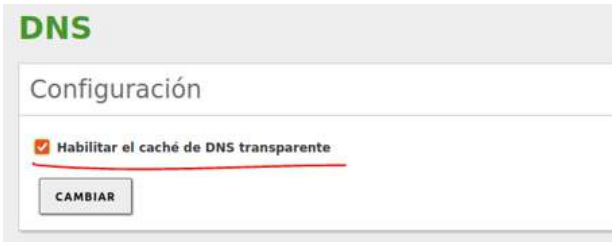

Figura 23. Habilitar el caché de DNS transparente

Se deben guardar los cambios, luego de realizar la habilitación del caché DNS transparente, y el sistema confirma que ya guardó los cambios realizados.

Figura 24. Guardando los cambios DNS

Para continuar con la configuración del servidor DNS, se debe agregar un dominio, como se puede observar en la siguiente imagen.

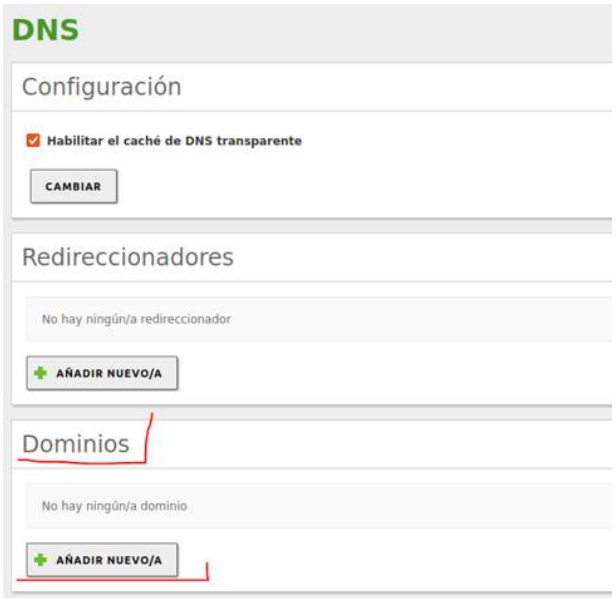

Figura 25. Agregar dominios en DNS Server

Luego de agregar el dominio, se puede observar que ya aparece en el listado de dominios del servidor DNS.

Figura 26. Dominio gioben-unad configurado en DNS Server

En esta imagen se puede observar que se agrega una dirección IP de dominio DNS 192.168.30.15.

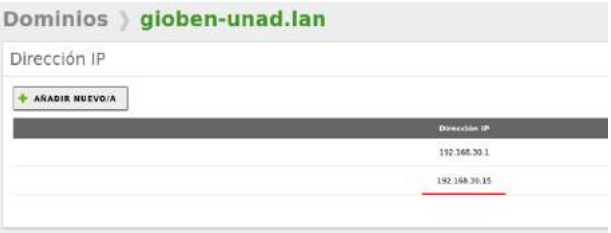

Figura 27. Dirección IP del dominio del servidor DNS

Estando en la máquina virtual Desktop, se puede observar que la dirección IP DNS ya aparece, como se puede observar en la siguiente imagen, DNS 192.168.30.15.

Figura 28. Evidencia de servicio DNS tomado por máquina virtual Desktop

CONTROLADOR DE DOMINIO

Para realizar esta configuración, se debe configurar nombre de máquina y dominó, en este caso se configura giobenunad, como se puede observar en la imagen.

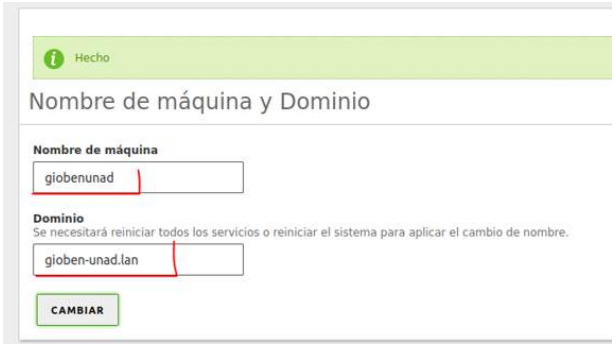

Figura 29. Asignación de nombre de máquina y Dominio

Se deben guardar los cambios realizados, y se confirma que, en la opción de Dominio, cargue el nombre de máquina antes configurado.

Figura 30. Verificación de nombre del dominio

Para realizar este proceso, antes se debe tener activo el servicio de DNS y controlador de dominio y compartición de ficheros como se puede observar en la imagen.

Figura 31. Configuración del estado de los módulos

Se deben activar estos servicios y se deben guardar los cambios realizados, como se puede observar en la imagen.

Figura 32. Guardando cambios de módulos

Se debe esperar que se complete el 100% del proceso de guardar los cambios.

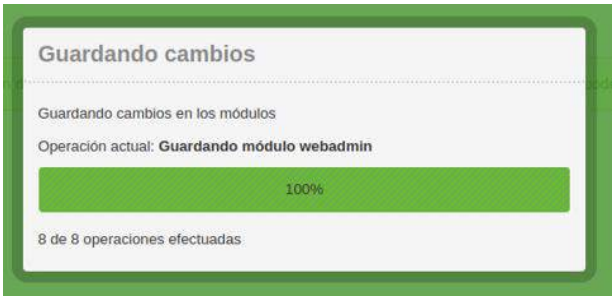

Figura 33. Proceso completado de guardando cambios de módulos

Luego de activar los módulos y guardar los cambios anteriores, en la opción de usuarios y equipos ya se puede añadir usuarios, en este caso se realiza la creación del usuario Angela, el cual pertenece al grupo de administradores de dominio.

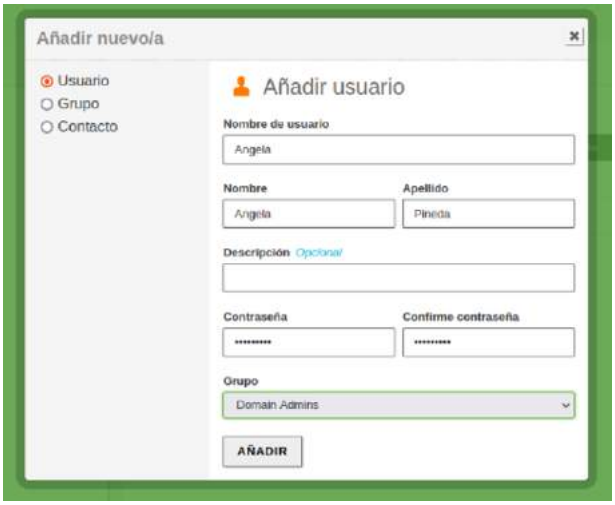

Imagen 34. Añadir usuario en el dominio creado

En esta imagen se puede observar que ya aparece el usuario que se creó en el paso anterior , y perteneciente al grupo de administrador de dominio.

Imagen 35. Verificación de usuario creado

El usuario que se crea también aparece en la lista de usuarios como se puede observar en la imagen.

Figura 36. Usuario creado aparece en el listado de usuarios

Y finalmente, en la máquina virtual Desktop ya se puede iniciar sesión con el usuario Angela, como se puede observar en la imagen final.

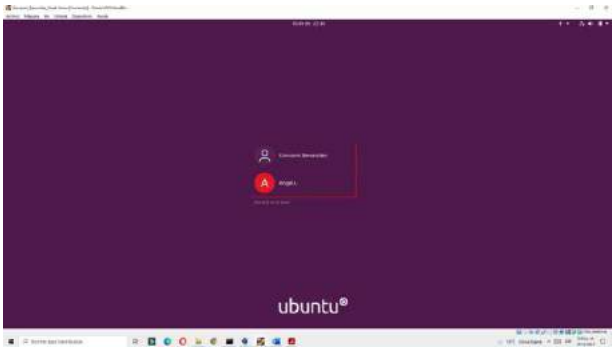

Figura 37. Acceso al usuario anteriormente creado en el dominio

3 TEMÁTICA 2

3.1 Proxy no transparente

Producto esperado: Implementación y configuración detallada del control del acceso de una estación GNU/Linux a los servicios de conectividad a Internet desde Zentyal a través de un proxy que filtra la salida por medio del puerto 1230.

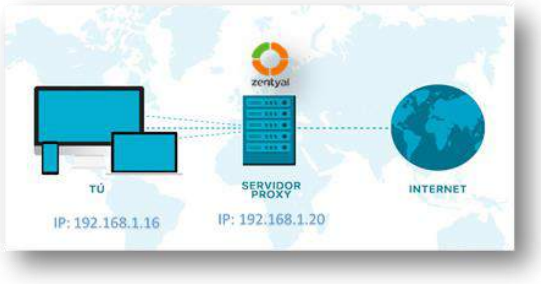

Figura 38 Configuración de la red

Se procede a configurar las interfaces de red del servidor debe contar con un direccionamiento estático para su configuración en cliente

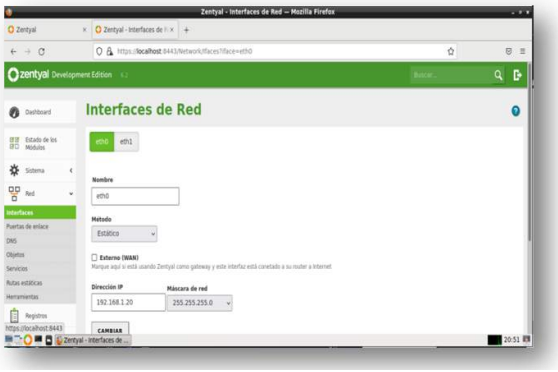

Figura 39 Interfaz eth0

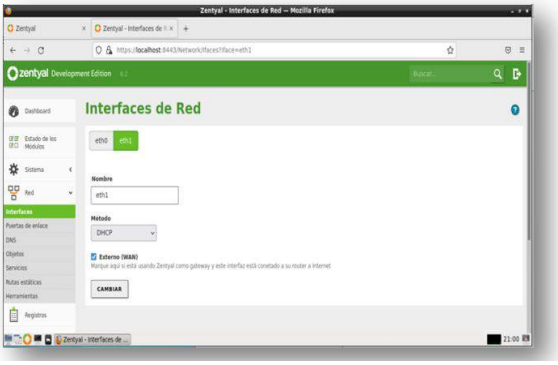

Figura 40 Interfaz eth1

Antes de iniciar la implementación y configuración, en el equipo cliente se valida navegación en el PC-Cliente.

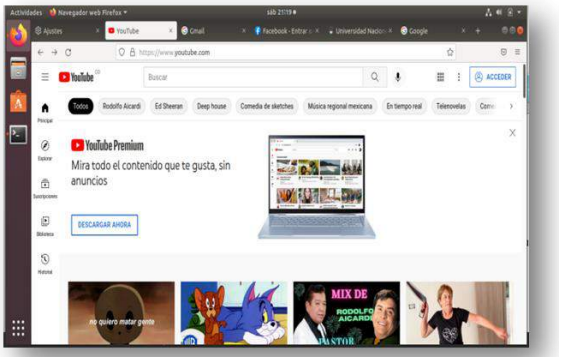

Figura 41 Navegación PC Cliente

También se realiza un ping a la ip del servidor para confirmar que hay comunicación entre el servidor y PC-cliente F

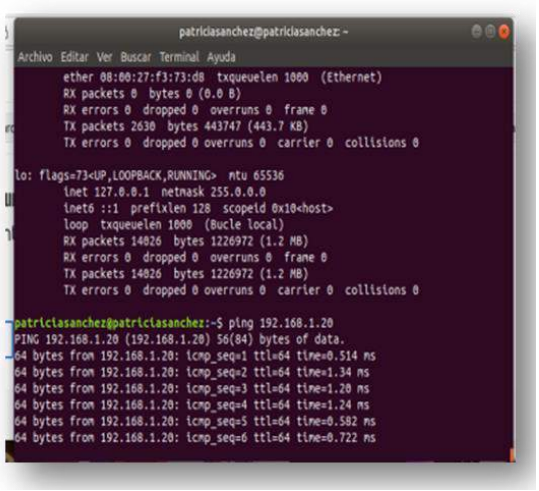

Figura 41 respuesta Ping a la ip del Servidor

Se procede a la activación del servicio Proxy HTTP por medio del menú de Estado de módulos (es necesario habilitarlo si no se encuentra activo)

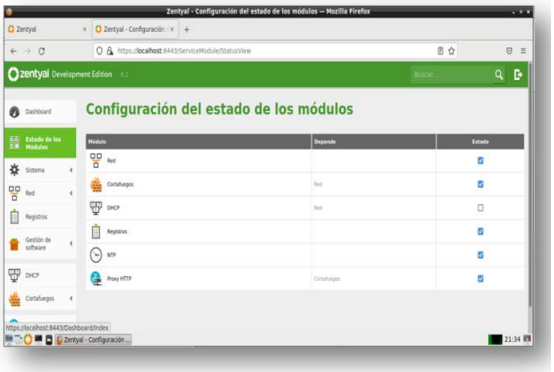

Figura 42 Módulo Proxy HTTP Activo

Posteriormente en la configuración general se indica el puerto 1230

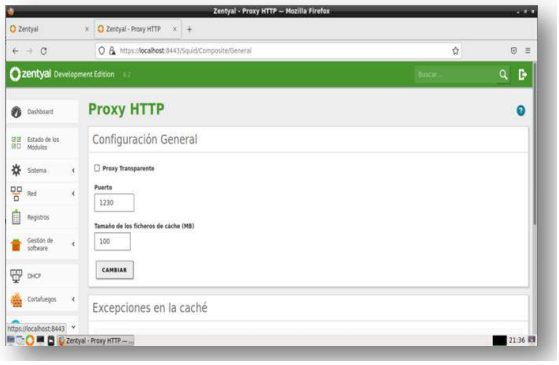

Figura 43 Configuración puerto 1230

Una vez hayamos decidido nuestra configuración general, tendremos que definir reglas de acceso. Por defecto, la sección Proxy HTTP Reglas de acceso contiene una regla permitiendo todo acceso.

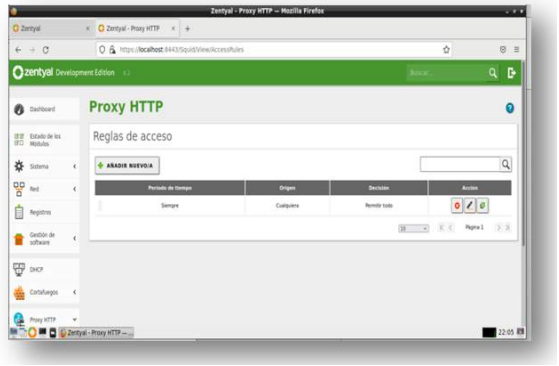

Figura 44 Reglas de acceso por defecto

Una de las formas de manejar proxy es permitir todo y denegar lo que se requiera o bloquear todo y permitir el acceso de las URL o dominio que se requiera

Para esto se crea un perfil de filtrado

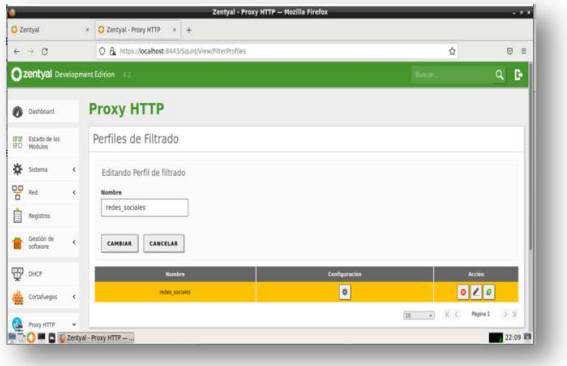

Figura 45 Creación de perfil

Posteriormente se configura el umbral y las URL sobre las cuales se va aplicar al perfil.

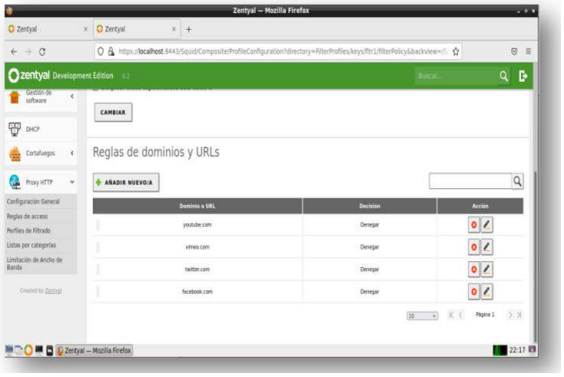

Figura 46 Reglas de dominio

Posteriormente en las reglas de acceso se aplica el perfil creado

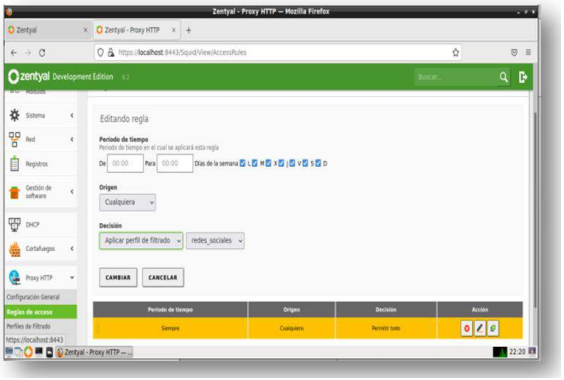

Figura 47 Aplicación de perfil

Dado a que la configuración del Proxy se ha realizado como no transparente se requiere la configuración en el navegador de equipo cliente

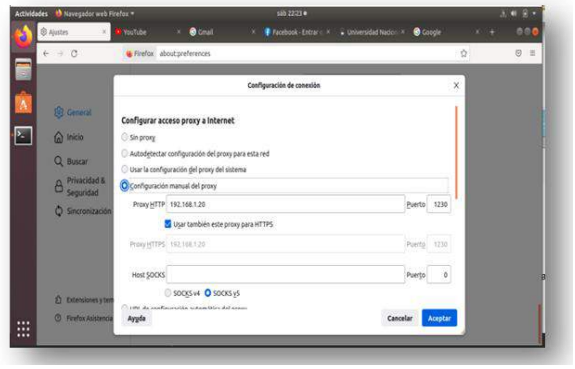

Figura 48 Configuración Proxy en PC-Cliente

Se procede a validar el cumplimiento de las reglas creadas

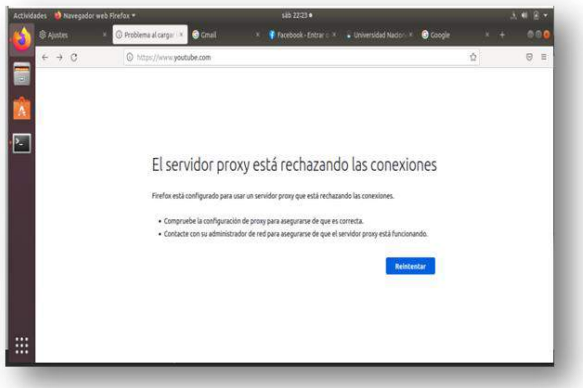

Figura 49 URL denegada

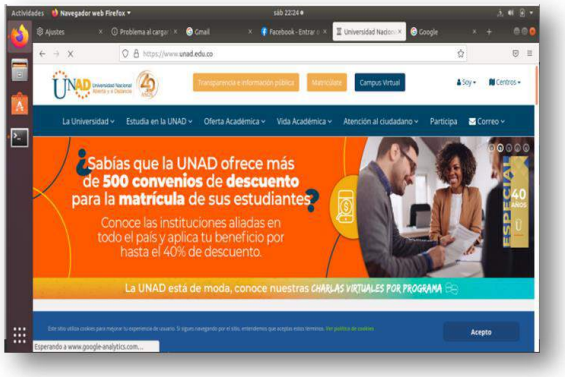

Figura 50 URL Permitida

4 TEMÁTICA 3

4.1 Cortafuegos

Producto esperado: Implementación y configuración detallada para la restricción de la apertura de sitios o portales Web de entretenimiento y redes sociales, evidenciando las reglas y políticas creadas. La validación

Como primer paso realizaremos la instalación del servidor Zentyal Server 6.2, en donde una de sus configuraciones principales en la máquina VirtualBox, corresponde a las tarjetas de Red las cuales deben ser configuradas de la siguiente manera:

Adaptador 1: Adaptador puente – (se selecciona el nombre del adaptador que proporciona el internet), tal como se muestra en el recuadro rojo

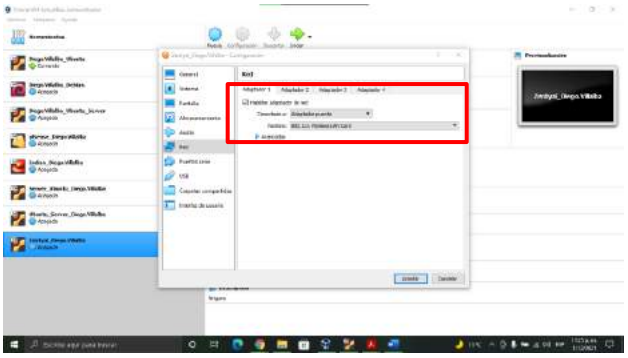

Figura 51 Configuración Adaptador 1 de red servidor

Adaptador 2: Seleccionamos la opción, Red interna y posteriormente le damos el nombre de LAN

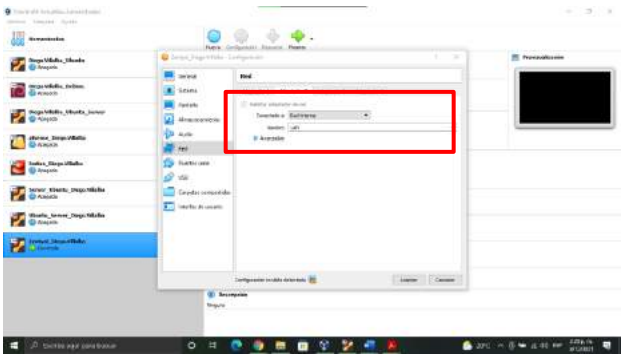

Figura 52 Configuración Adaptador 2 de red servidor

Configuración tarjeta de red máquina Desktop y/o Cliente

Adaptador 1: Para la máquina correspondiente al cliente, solo configuraremos un adaptador, el cual seleccionamos Red interna y le damos el nombre de LAN

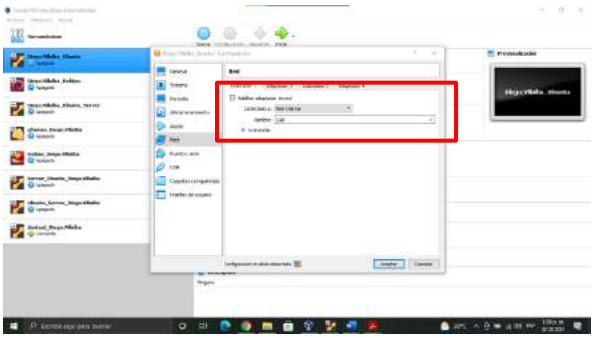

Figura 53 Configuración Adaptador 1 de red cliente

Ingresado al sistema, comenzaremos con la configuración inicial para la administración de recursos mediante Zentyal

Figura 54 Configuración inicial Zentyal

Como primera medida y para el desarrollo de la temática seleccionada, instalaremos en el menú de paquetes de Zentyal en **Firewall**.

Figura 55 Instalación Firewall

Una vez instalado los paquetes necesarios para la configuración del cortafuego nos disponemos a configurar los tipos de interfaces las cuales quedarán de la siguiente manera:

- **Eth0** = External
- **Eth1** = Internal

Figura 56 Configuración interfaces de red

Continuamos realizando la configuración de la interfaz de la siguiente manera:

- **Eth0** = DHCP para tipo externa WAN
- **Eth1** = Static para tipo interna LAN

Dirección IP: 192.168.0.22
Máscara de red: 255.255.255.0

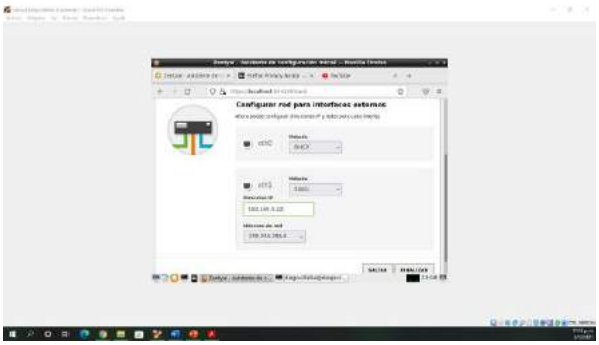

Figura 57 Configuración de direcciones ip en interfaces

Posteriormente vemos el panel principal del Dashboard, con los paquetes instalados en el menú del costado izquierdo.

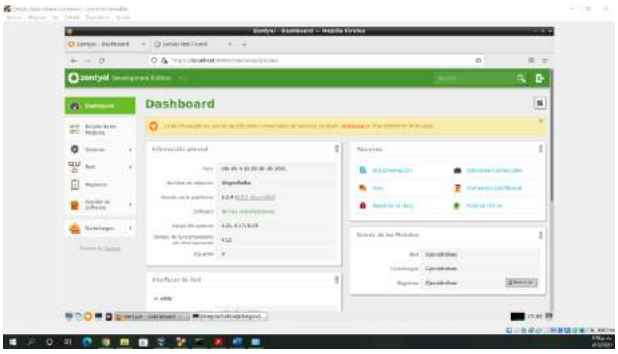

Figura 58 Configuración Adaptador 2 de red servidor

Como primera medida realizamos la verificación de conexión de red mediante terminal, la cual haremos un ping hacia los DNS de Google: ping 8.8.8.8
Como resultado nos muestra que no tenemos red, tal como se aprecia en la siguiente imagen. Lo cual es bueno porque desde un principio el firewall bloquea las conexiones externas lo cual permite dar seguridad al sistema y la red interna

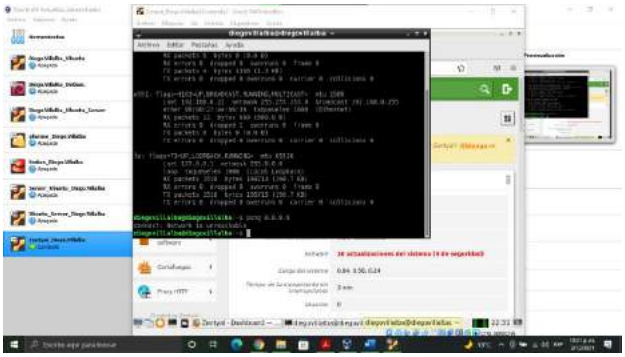

Figura 59 Verificación de conexión vía terminal

Como primera medida realizaremos la configuración de la red, la cual nos permitirá abrir las conexiones tanto externas como internas, para ello nos dirigimos a la pestaña de Registro, la cual se puede observar en la imagen dentro del recuadro **Rojo,** posteriormente seleccionamos la opción Configurar los registros, la cual se puede apreciar en el recuadro **Azul** y enseguida habilitamos las casillas de los dominios que se muestran en la imagen denominados:

- Cambios en la configuración, Sesiones del administrador
- Cortafuegos

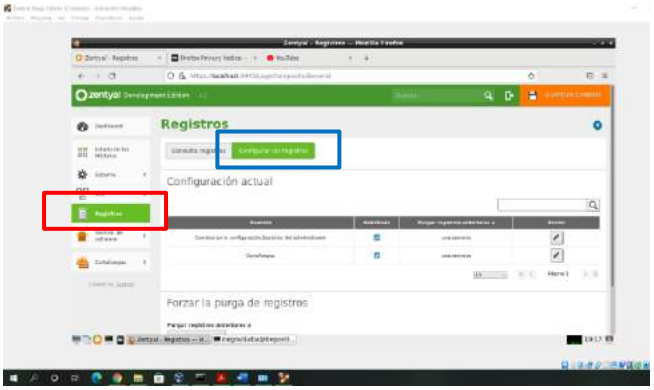

Figura 60 Registro de conexiones de red

Posteriormente nos dirigimos a la opción de **Red** y seleccionamos **Interfaces**, las cuales configuraremos de la siguiente manera:

- **Eth0 =** Se cambia el nombre a WAN y se realiza el cambio por la dirección IP **192.168.0.122** con mascara de red de 25 bit, la cual corresponde a **255.255.255.128**, es importante mencionar que la casilla **Externo (WAN)**, para que el sistema toma que esta interfaz actúa de modo externo de lo contrario los tomara como una red interna.

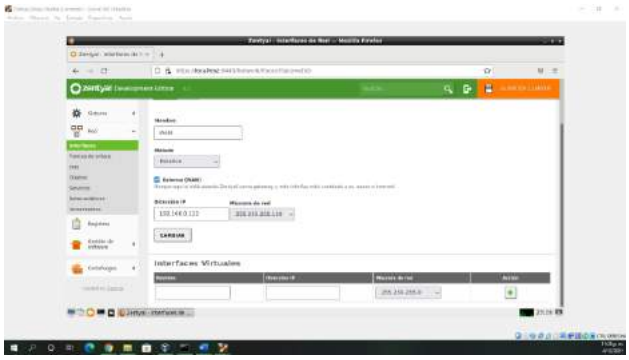

Figura 61 Configuración de interfaz red WAN

- **Eth1 = Cambiaremos** el nombre de la interfaz a LAN para determinar que esta interfaz corresponde a la red interna y trabajara con la IP **192.168.200.254**, para configurar desde otro segmento de red.

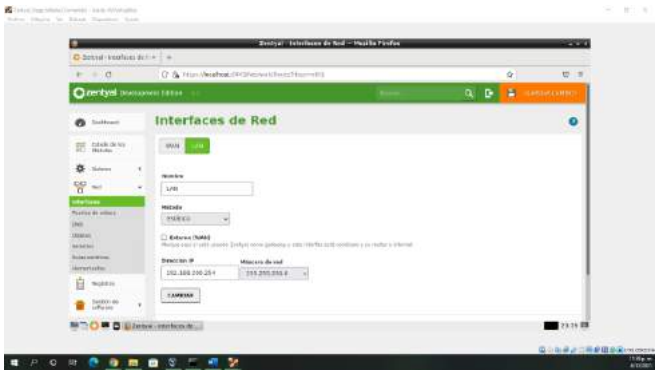

Figura 62 Configuración de interfaz red LAN

En seguida ingresamos a la opción de **Puerta de enlace**, señada en el recuadro rojo, la cual al configurar la red LAN de manera estática debemos crear una nueva puerta de enlace para ello daremos clic en el botón **añadir nuevo**

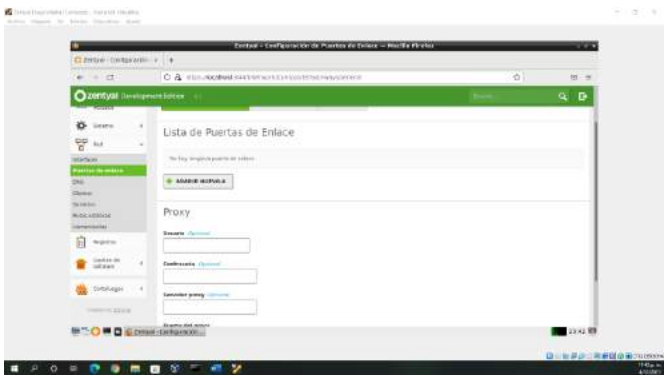

Figura 63 Configuración puerta de enlace red LAN

La configuración de la nueva puerta de enlace se realiza de la siguiente manera:

- Nombre: gw-wan
- Dirección IP: 192.168.0.1 (que es la que tenía anteriormente)

Finalmente se debe habilitar la casilla predeterminado y damos clic en el botón añadir, tal como se muestra en la siguiente imagen

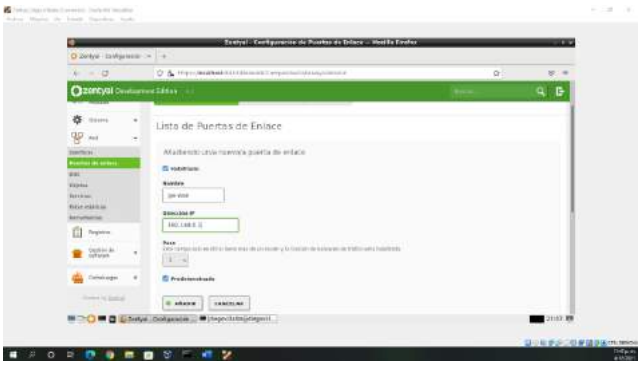

Figura 64 Asignación Ip puerta de enlace red LAN

Como podemos ver en la imagen a continuación la nueva puerta de enlace ha sido creada y para terminar este proceso damos clic en el botón guardar que se encuentra en la parte superior derecha el cual es de color naranja, para que el sistema guarde y aplique los cambios realizados

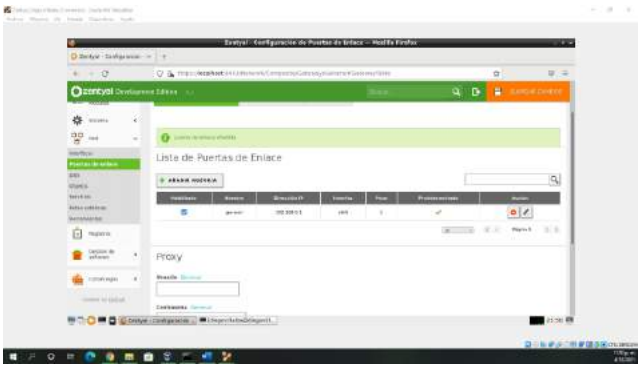

Figura 65 Configuración puerta de enlace red LAN

Continuando con el proceso de instalación, ahora nos dirigimos a la opción de DNS, demarcada por el cuadro **Rojo**. Donde de igual manera debemos realizar la creación de un nuevo dominio por la configuración estática de la red LAN

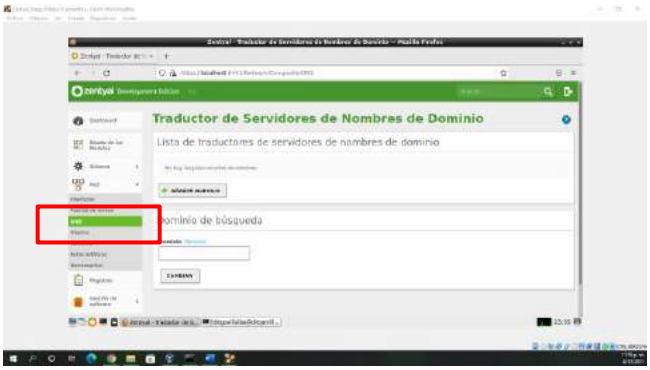

Figura 66 Configuración de DNS a red LAN

Para dicha configuración utilizaremos la configuración dando clic en el botón **añadir nuevo**, y utilizaremos los siguientes nombres de dominio:

- **8.8.8.8 y 1.1.1.1**

Los cuales son de Google y los usaremos para efectos de pruebas para este ejercicio. Para finalizar damos clic en el botón guardar para aplicar los cambios realizados.

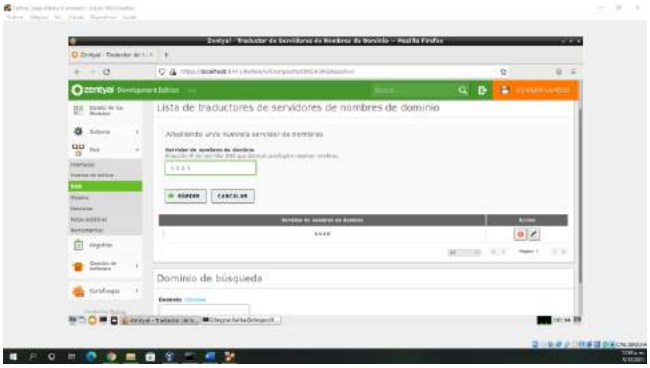

Figura 67 Asignación de nombre domino a DNS

La operación antes mencionada se puede validar realizando un ping hacia el dominio: www.google.hn, donde podemos observar que efectivamente el DNS se está comunicando con dicho dominio de manera exitosa. Ya con esto damos por terminada la configuración de red la cual es requerida para realizar posteriormente la configuración del firewall junto con su administración.

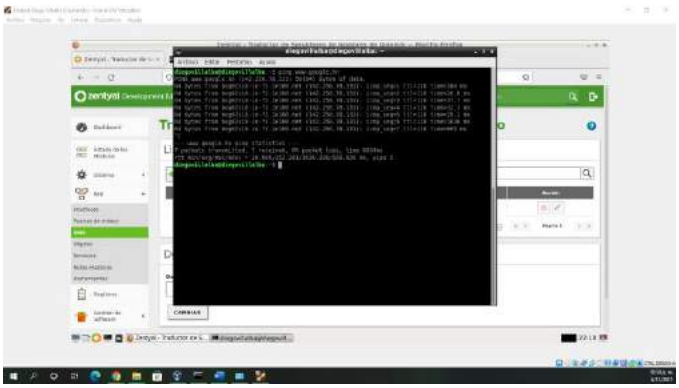

Figura 68 Validación de conexión por terminal

Para iniciar la configuración de servicios y negación de acceso a sitios web mediante el firewall como primer paso ingresamos al servidor, mediante el uso de un equipo cliente o desktop, el cual para nuestro ejercicio trabajaremos con uno usando el sistema operativo **GNU/Linux Ubuntu** y a través del navegador usaremos la siguiente dirección https://192.168.200.254:8443/, para dar ingreso al Dashboard de Zentyal tal como se muestra en la siguiente imagen.

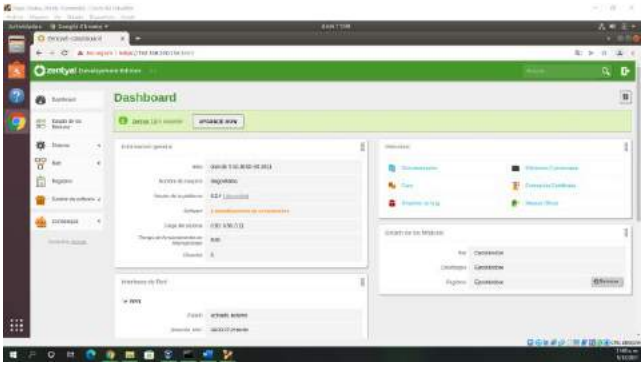

Figura 69 Conexión a Zentyal por terminal cliente

Ahora bien, para realizar la restricción de acceso a páginas o portales web de entretenimiento y redes sociales, debemos crear un nuevo objeto en el menú desplegable de la opción **Red**, allí creamos un nuevo objeto el cual, para este ejercicio llamare Facebook - Instagram.

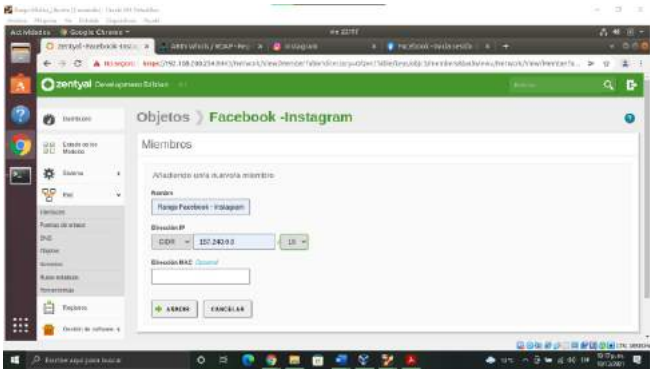

Figura 70 Configuración de objetos

Dicho objeto se configura de la siguiente manera. Como primera medida debemos hallar o encontrar la dirección de Ip pública del sitio web al cual vamos a denegar los servicios de acceso, para ello haremos uso de la terminal de nuestro equipo desktop cliente y en ella haremos un ping a la dirección del sitio web al cual deniega el servicio tal como se puede observar en la siguiente imagen.

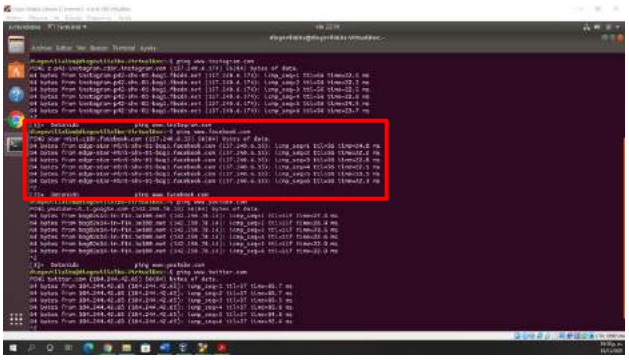

Figura 71 Ping a Facebook para detectar ip pública

Como pudimos ver en la imagen anterior al hacer ping a la dirección **www.facebook.com.** La terminal nos muestra la dirección Ip pública de Facebook la cual es 157.240.6.35, posteriormente hacemos uso de la página web: **search.arin.net**, en la cual podremos encontrar el rango de la Ip pública tal como se muestra en la siguiente imagen señalada en recuadro **Rojo.**

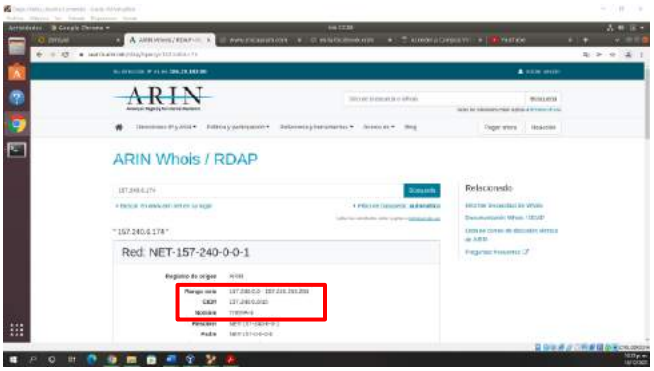

Figura 72 Ingreso a pagina ARIN

Una vez obtenido el rango CIDR de la dirección ip para Facebook, la asignaremos en el nuevo objeto configurado tal como se muestra en la imagen a continuación.

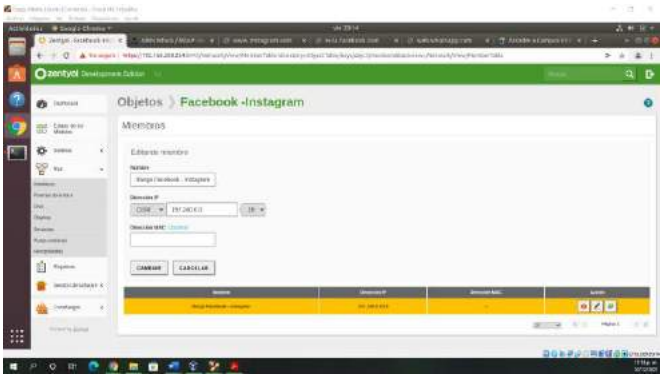

Figura 73 Configuración de ip publica a objeto

Después de la configuración de los objetos, nos dirigimos al cortafuegos en la opción **Filtrado de paquetes** y seleccionamos la **Regla de filtrado para las redes**

internas, para iniciar la configuración de la negación del servicio de Facebook

Figura 74 Ingreso a reglas de firewall

Al ingresar a la regla mencionada, añadimos una nueva regla de filtrado la cual configuraremos como:
Decisión: Denegar
Origen: Cualquiera
Destino: Objeto destino para los cual elegimos el que creamos anteriormente **Facebook-Instagram**
Servicio: Cualquiera
Descripción: Denegar servicios de meta, ya que Facebook cambió su nombre a **Meta**, todas sus plataformas como Instagram Facebook y WhatsApp utilizan el rango de ip 157.240.0.0/16

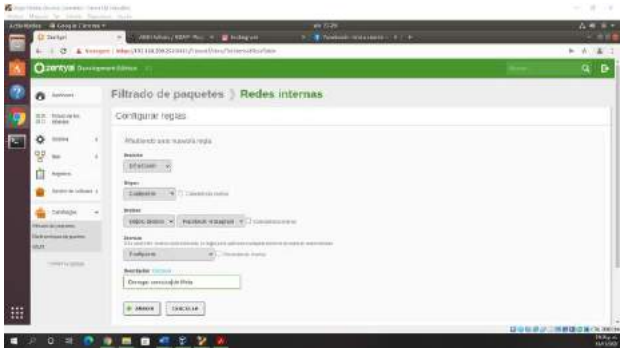

Figura 75 configuración de nueva regla en el firewall

Terminada la configuración de la regla para denegar servicios, podemos ver que está ya está activa y funcionando.

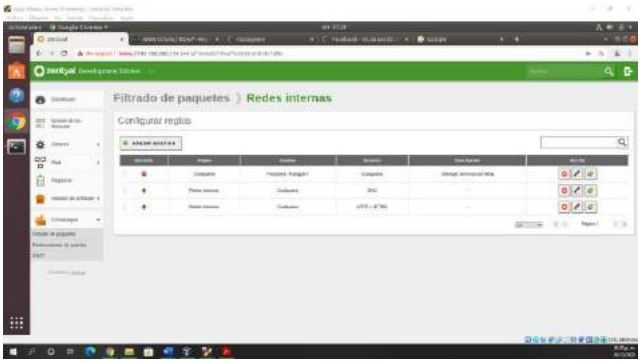

Figura 76 Uso de la nueva regla configurada

Comprobamos que efectivamente los servicios han quedado correctamente configurados en el cortafuegos, ya que no podemos tener acceso a las páginas de Instagram y Facebook, tal como se evidencia en las siguientes imágenes.

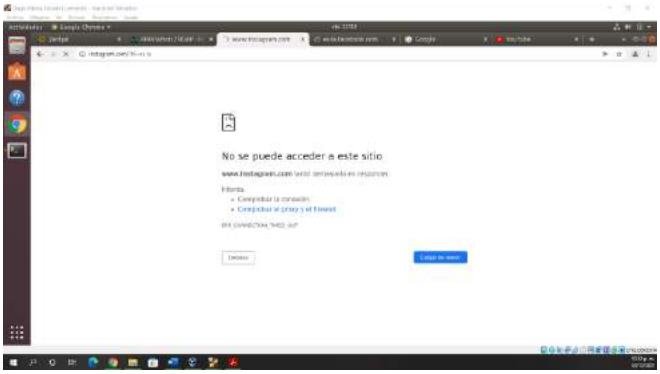

Figura 77 Acceso denegado a Facebook

De igual manera, podemos evidenciar que tenemos conexión a otras páginas, para ello lo podemos verificar ingresando al campus virtual de la UNAD. Donde podemos ver el ingreso normal a este.

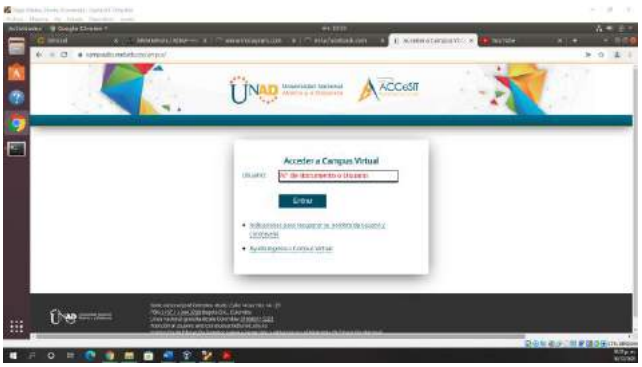

Figura 78 Ingreso a aula virtual UNAD

Es importante mencionar que estas mismas configuraciones, se realizan para denegar el acceso a cualquier portal ya sea de entretenimiento, como Netflix o todas las redes sociales y demás portales web que el usuario o entidad desee restringir su acceso por parte de los desktops o clientes conectados a la red LAN administrada por el servidor.

Con esto se daría fin al desarrollo de la actividad paso 8 correspondiente a la Temática 3, donde se realizó la configuración del servidor firewall Zentyal junto con la debida explicación para realizar la negación de acceso a portales web de entretenimiento y redes sociales.

1 TEMÁTICA 5

1.1 VPN

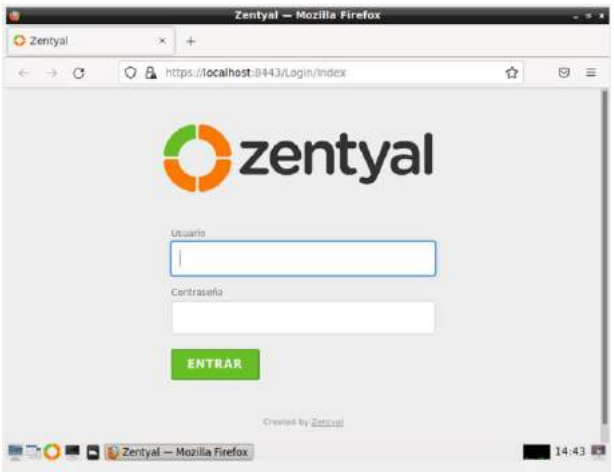

Figura 79 Login de Zentyal

Realizamos la configuración del sistema Operativo, ingresamos con usuario y contraseña descrita en la instalación del sistema.

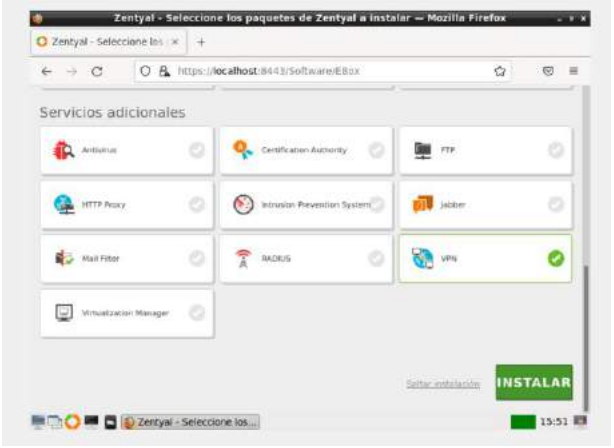

Figura 80 Panel principal de Zentyal

Nos muestra las opciones de configuración e instalación de los diferentes módulos que nos entrega el sistema, para este caso seleccionamos VPN.

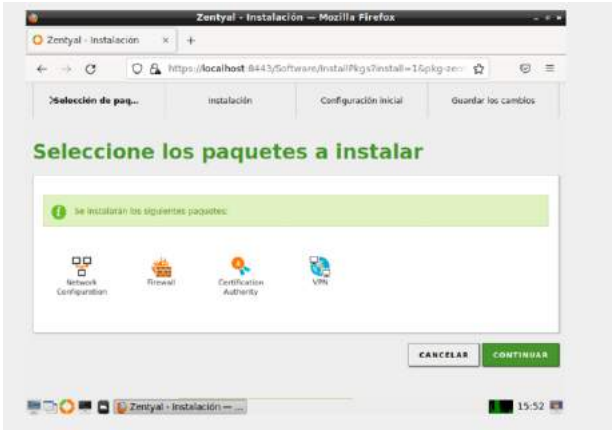

Figura 81 Selección de instalación de VPN

Después de seleccionados nos indica cuáles son los módulos que se instalarán y el orden de los mismos.

Figura 82 Cargue de instalación Zentyal

Se inicia la instalación de los módulos seleccionados.

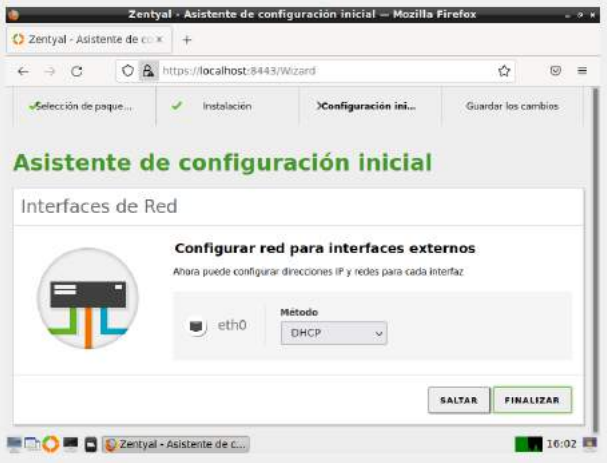

Figura 83 Configuración de DHCP

Seleccionamos la configuración que deseamos para la RED, en este caso se realizará por DHCP.

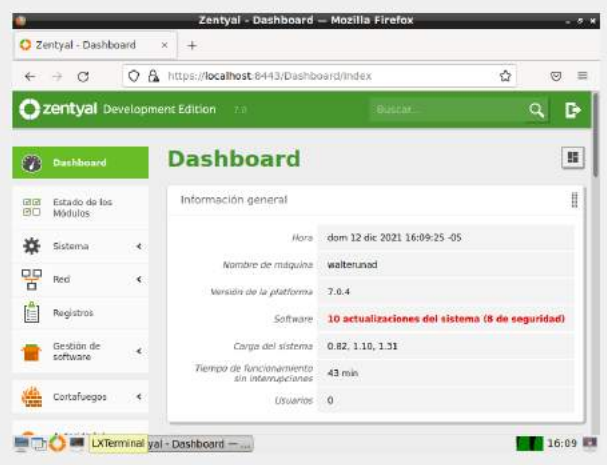

Figura 84 Interface inicial de configuración

Nos muestra la interfaz inicial e iniciamos el proceso de configuración.

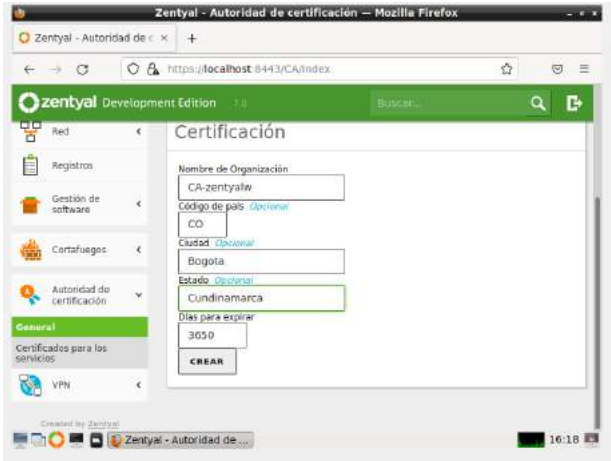

Figura 85 Generación de certificados

Generamos los certificados de confianza de las máquinas

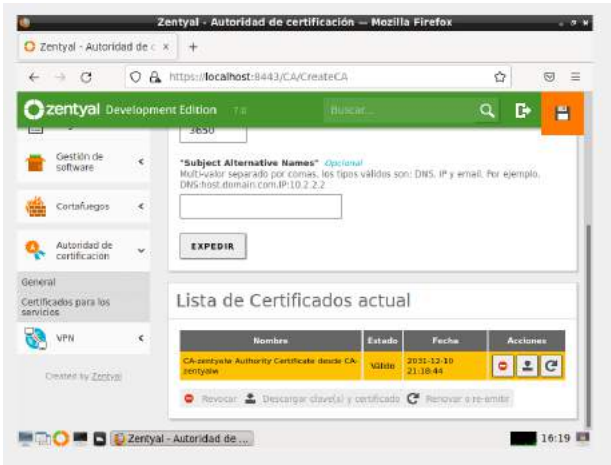

Figura 86 Configuración de certificados

Configuramos y revisamos los certificados, el sistema antes de realizar el servidor de VPN nos solicita que realicemos la configuración de certificados.

Figura 87 Configuración servidor VPN

Después de crear los certificados, se realizará la configuración del servidor de VPN. colocamos los el nombre que deseamos.

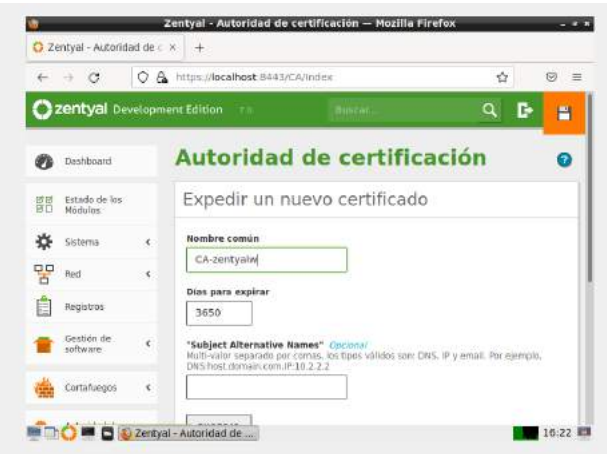

Figura 88 Creación de certificado por usuario

Después de esto nos solicitará realizar la creación de un certificado para usuario este es el certificado que se debe entregar al usuario y el cual debe descomprimir e instalar en el sistema operativo que tenga el cliente final.

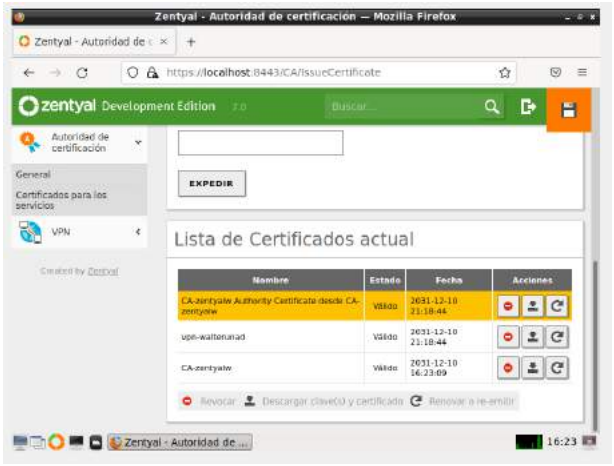

Figura 89 Listado de certificados seguros

Este es el listado de certificados seguros generados para nuestras conexiones hacia el servidor de VPN.

Figura 90 Configuración rangos DHCP

Configuramos los rangos por DHCP que estaremos bloqueando.

Figura 91 Configuración proxy de conexión

Configuramos el Proxy de conexión y los puertos de conexión de los mismos, con esto garantizamos que la VPN y todo el tráfico que pase por este se bloqueará y tendremos filtros de conexión de diferentes dispositivos de conexión por nuestro servidor de Zentyal.
Se configuran las reglas de acceso a las páginas que deseamos bloquear o permitir

4.1.1 Conclusiones.

- En este trabajo se configura GNU/Linux Zentyal Server 6.2 (Instalar y configurar Zentyal Server como sistema operativo base para disponer de los servicios de Infraestructura IT).
- Se instala y configura DHCP Server, DNS Server y Controlador de Dominio.
- Se configuran máquinas virtuales para la puesta en marcha de servicios, para brindar soluciones alternativas a clientes.
- Se realiza la implementación y configuración detallada del acceso de una estación de trabajo GNU/Linux a través de un usuario y contraseña, así como también el registro de dicha estación en los servicios de Infraestructura IT de Zentyal.
- Mediante las herramientas firewall se declararon las reglas y/o políticas necesarias para la denegación de accesos a los sitios web mencionados

5 REFERENCIAS

[1] Firewall — Zentyal 7.0 Documentation. Zentyal.Org. Retrieved December 11, 2021, from https://doc.zentyal.org/en/firewall.html
[2] Community - Zentyal Linux Server. (2019, January 16). Zentyal.Com. https://zentyal.com/community/
[3] Primeros pasos con Zentyal — Documentación de Zentyal 7.0. (n.d.). Zentyal.Org. Retrieved December 11, 2021, from https://doc.zentyal.org/es/firststeps.html
[4] Zentyal Server | Instalación y primeros pasos DETALLADOS para ti. (2018, April 8). YouTube. https://www.youtube.com/watch?v=tG_NHAUYUbU
[5] Inicio - Zentyal Linux Server. (2019, February 7). Zentyal.com. https://zentyal.com/es/inicio/
[6] Guzmán, D. A. (29 de 11 de 2021). meet.google.com. Obtenido de meet.google.com: https://bit.ly/3Ed73xe.
[6] Murillo, R. (23 de 05 de 2020). www.youtube.com. Obtenido de www.youtube.com: https://www.youtube.com/watch?v=I-2fw_5BZhs

.