IMPLEMENTACIÓN CON GNU/LINUX ZENTYAL SERVER

Hermes Castañeda Pernett
e-mail: hscastanedap@unadvirtual.edu.co
Clara Milena Castillo Salmanca
e-mail: cmcastillo@unadvirtual.edu.co
Leonardo Puerto Layton
e-mail: jlpuertol@unadvirtual.edu.co
Alberth Fabián Perez Mendivelso
e-mail: afperem@unadvirtual.edu.co
Néstor Augusto Tocancipá Guevara
e-mail: natocancipag@unadvirtual.edu.co

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

PALABRAS CLAVE: Zentyal Server, conectividad, DHCP, cortafuegos, File Server, Print Server.

1 INTRODUCCIÓN

Este articulo exhibe la instalación, configuración y administración GNU/Linux Zentyal Server de alto rendimiento, seguridad y estabilidad acorde a las necesidades empresariales. Aborda los servicios de la red de computadores con bloqueos y permisos de acceso en las comunicaciones, la implementación se enfoca en una solución segura y en el resguardo de la información sensible con un controlador de dominio que administra las credenciales en el inicio de sesión y actúa con un filtro entre la conexión a internet, restricción de los servidores y la comunicación en la red verificando las conexiones de forma segura, aísla las diferentes redes con una zona perimetral segura que protege las consultas hacia internet con un proxy que asigna un certificado aceptado por el cliente para dar continuidad a la comunicación o una alerta de conexión insegura, redirige los puertos en los protocolos, instaura un conjunto de políticas de filtrado de tráfico y regula el uso de los otros puertos definidos en un cortafuego.

2 MARCO TEORICO

2.1 GNU/LINUX ZENTIAL SERVER

El servidor de red Zentyal bajo una distribución GNU/Linux se basa en Ubuntu 18 para administrar los principales servicios de la red informática, controla el acceso a Internet brindando seguridad en las comunicaciones red mediante el navegador web.

2.2 PROCESO DE INSTALACIÓN

GNU/Linux Zentyal se integra con módulos configurables actuando en la red, la fuente del instalador se aloja en su sitio web con el enlace de zentyal-6.2-development-amd64.iso. Al completar la descarga se define la configuración de la maquina virtual e inicia la instalación fijando la zona horaria (Fig. 1) y teclado.

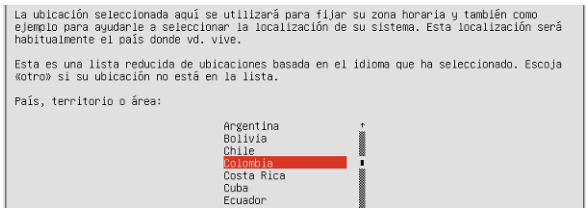

Figura 1. Zona horaria en la instalación Zentyal .

Luego se asigna el nombre del servidor en la red local, la configuración del usuario, el proxy HTTP para acceder a la red, el cargador de arranque GRUB en el registro principal y la hora local del sistema.

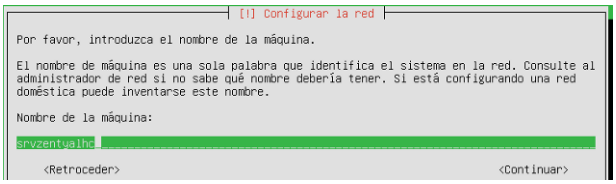

Figura 2. Hostname.

Finalizada la instalación se acepta la advertencia del certificado autofirmado en la Fig. 3 accediendo al puerto 8443 en el navegador, así https://127.0.0.1:8443/

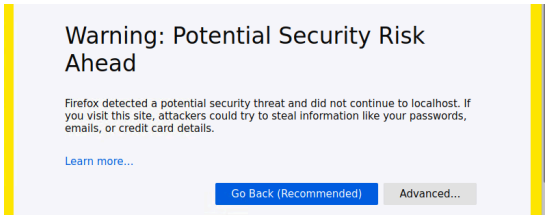

Figura 3. Ingreso a GNU/Linux Zentyal Server.

3 DHCP SERVER, DNS SERVER Y CONTROLADOR DE DOMINIO

La implementación de los servicios en la red se despliega con la configuración del firewall donde se define el tipo de interfaz interna o externa, la primera con los recursos de la red local y la segunda con el acceso de Internet representando en la Fig 1, en la interfaz eth1 con dirección IP 192.168.100.1 para DHCP, eth2 con dirección IP 192.168.200.1 con la zona perimetral para reguardar los servidores locales a través del sistema de seguridad Endian especializado en cortafuegos.

Figura 1. Configuración de las interfaces de red

La IP 10.0.2.2 dada a la puerta de enlace interconecta las redes a través de los protocolos y otorga acceso a Internet en los equipos de red local LAN con una única conexión a Internet traduciendo las solicitudes de los nombres de host y de dominio de las direcciones IP con los DNS fijados.

Figura 2. Gateway

3.1 CONFIGURACIÓN DE DNS SERVER

El sistema de nombres de domino DNS sistematiza la resolución de nombres en las redes, apunta a los dominios del servidor correspondiente y traduce la dirección IP el nombre del dominio.

Finalizada la instalación de los módulos en la Fig. 3 se verifican las reglas de filtrado de los protocolos correspondientes a ICMP para el control de mensajes de Internet, que responde a ping, TCP de control de transmisión para la comunicación dentro de la red, UDP protocolo de datagramas de transporte basado en el intercambio de envío en la red sin establecer una conexión entre el emisor y el receptor y HTTP de transferencia de hipertexto, protocolo de comunicación para las transferencias de información en internet.

Figura 3. Instalación de módulos

El servidor DNS usa la caché de las consultas desde las redes internas no configuradas directamente en Zentyal con rutas hacia segmentos internos o en redes VPN con la consulta de las zonas de DNS locales cuando están presentes; el servidor DNS autoritario establece la resolución de cada petición y las almacena localmente durante un período de tiempo aumentando la sensación de velocidad de los usuarios y reduciendo el consumo de tráfico hacia Internet.[1]

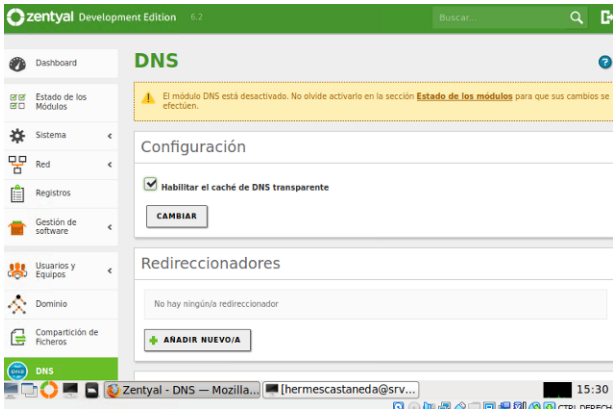

Figura 4. Caché de DNS

Los redireccionadores reenvían las consultas que buscan la cache local compuesta de los dominios registrados y las consultas cachedas; si no hay registro acude a los servidores de DNS asignados.

Figura 5. Redirectores DNS

El DNS autoritario responde a las consultas de los dominios asignados y resuelve los dominios con el servidor caché por las consultas de una red interna.

En la configuración del dominio de búsqueda hermescastaneda.zentynal se elimina la dirección IP de la interface eth0 correspondiente a la WAN.

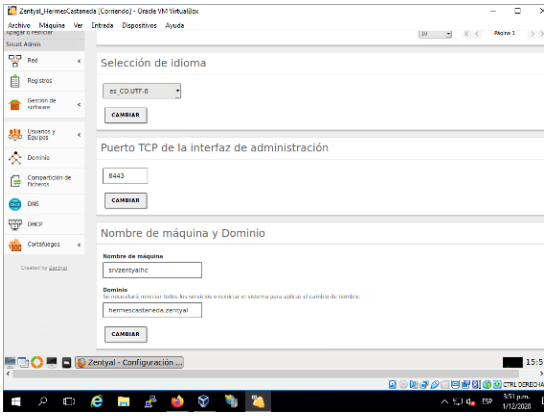

Figura 6. configuración de DNS

3.2 CONFIGURACIÓN DE NTP

El protocolo de internet sincroniza los relojes de los sistemas usando la capa de transporte UDP con el puerto 123, usualmente por DHCP.

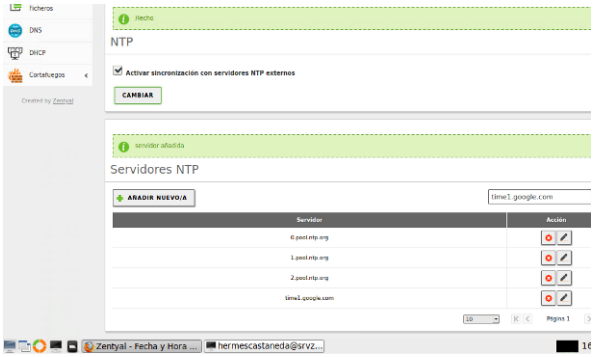

Figura 7. Servicio NTP

Los objetos de red representan un elemento o conjunto en la red simplificando la gestión de la configuración del filtrado de paquetes en el firewall hacia los servicios DNS, DHCP y NTP.[1]

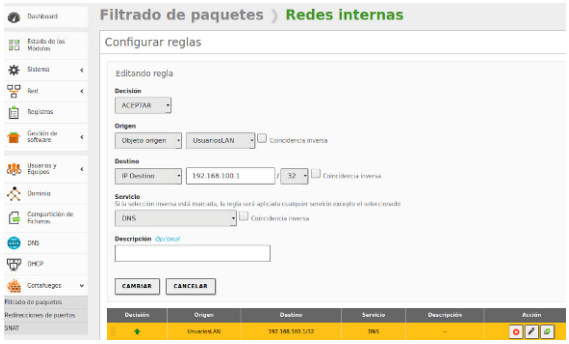

Figura 8. Reglas de filtrado en el firewall

3.3 CONFIGURACIÓN DHCP SERVER

Al habilitar la interface de red el servidor DHCP da automáticamente las direcciones de red, el modelo cliente servidor solicita la configuración IP al servidor y recurre a una base de datos que contiene la información de red asignable. La puerta de enlace comunica los destinos no presentes en la red local, el dominio de búsqueda resuelve el nombre, para resolver un nombre de dominio usa el servidor DNS con el servidor de nombres secundario cuando el primario no está disponible, el servidor NTP sincroniza el reloj del sistema y el servidor WINS resuelve el nombre en una red NetBIOS.[1]

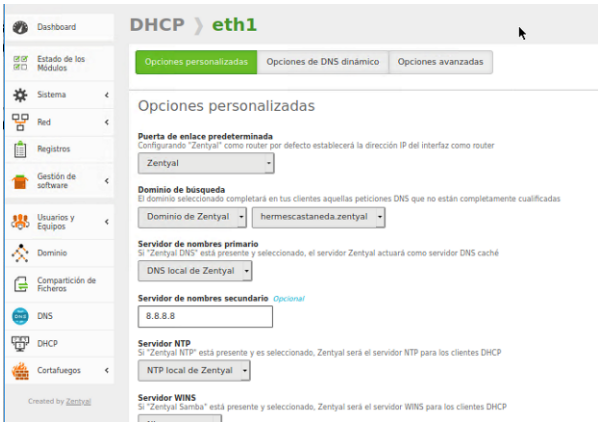

Figura 9. Configuración DHCP

En la opciones de configuración del servicio DHCP se fijan los rangos de direcciones IP disponibles para asignar en la interfaz de red.

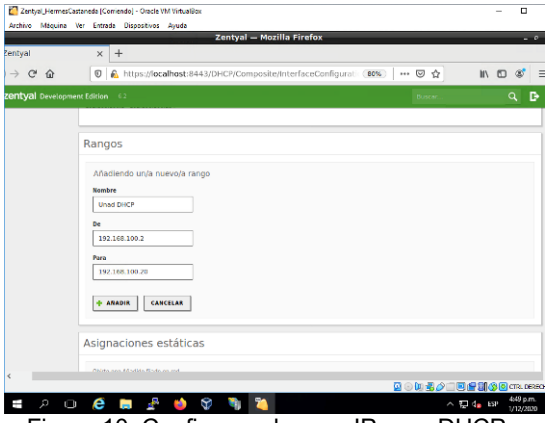

Figura 10. Configurar el rango IP para DHCP

El DNS dinámico asigna los nombres de dominio a los clientes DHCP mediante la integración de los módulos de DHCP y DNS; facilita el reconocimiento de los ordenadores presentes en la red por medio de un nombre de dominio único en lugar de una dirección IP.[1]

Los tiempos de asignación del servidor DHCP definen la renovación de la dirección IP con un tiempo que expira según lo indicado para la renovación.

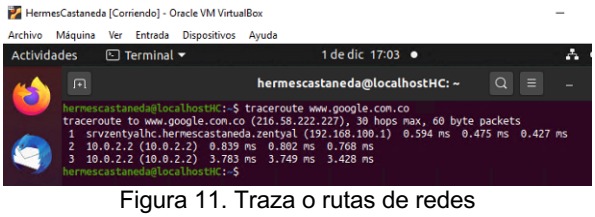

Figura 11. Traza o rutas de redes

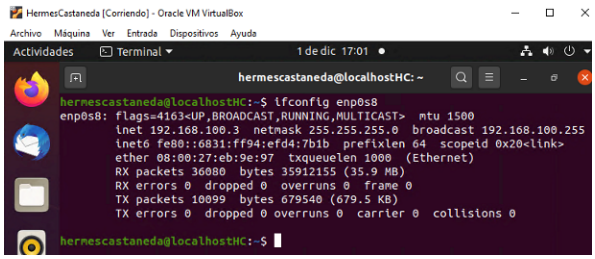

Figura 12. Traza o rutas de redes

3.4 CONTROLADOR DE DOMINIO

El controlador de dominio Zentyal integra samba, es una alternativa del Directorio Activo de Microsoft, uso del protocolo ligero de acceso a directorios LDAP, servidor DNS y la autenticación distribuida mediante Kerberos. [2]

Figura 13. Configuración Dominio

Al habilitar el modulo del controlador de dominio, se asigna la cuota de espacio en disco del usuario, la unidad organizativa, el contenedor de otros objetos en la unidad organizativa definiendo los grupos, usuarios y otras unidades organizativas, la estructura de datos establece el árbol y las diferentes políticas aplicadas a cada nodo.

En la raíz del árbol se aprecia el dominio local hermescastaneda.zentyal conformado por las unidades organizativas definidas y los equipos enlazados al dominio, los grupos de la organización, usuarios de la organización y servidores que replican la información del directorio, puede asumir los diferentes roles a nivel de bosque FSMO de un dominio.

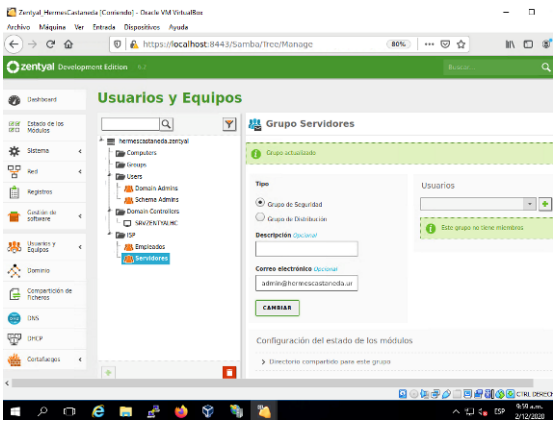

Figura 14. Unidad organizativa

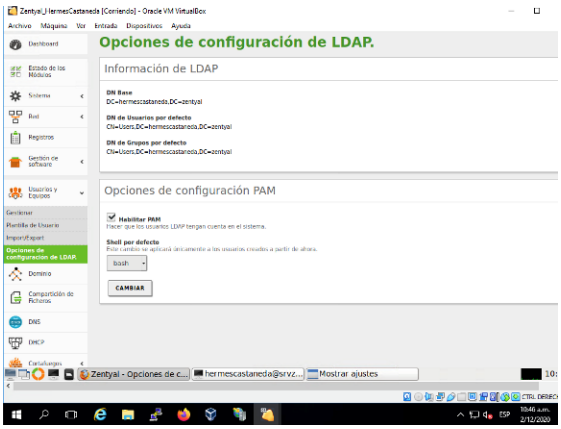

Figura 15. Configuración Dominio

Para integrar Ubuntu Server al dominio requiere de los servidores de nombres DNS y la instalación de pbis-open para unirse al dominio. PBIS es un software que se enlaza el dominio con inicio de sesión y utiliza permisos en samba.

Unión al dominio la ejecución del comando domainjoin-cli join hermescastaneda.zentynal hermes

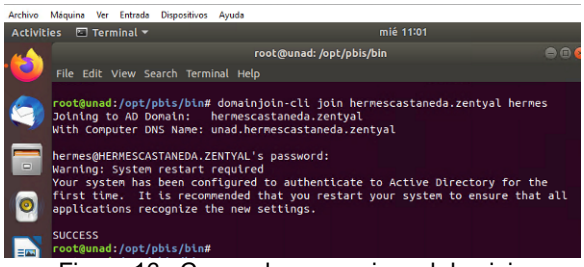

Figura 16. Comando para unirse al dominio

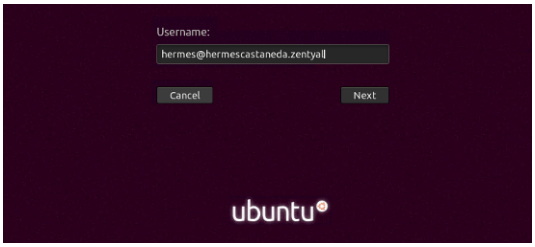

Figura 17. Acceso de Ubuntu Server en el dominio

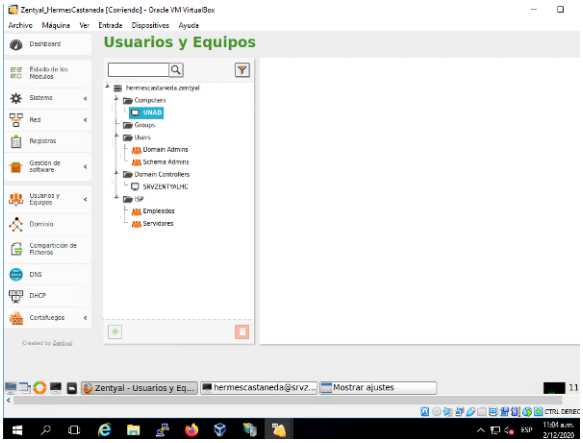

Figura 18. Registro de la estación

4 PROXY NO TRANSPARENTE

Los paquetes requeridos para la configuración del proxy transparente son los siguientes:

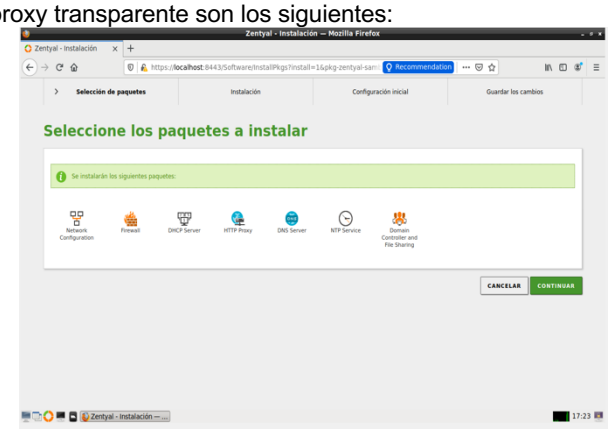

Figura 19. Instalación de módulos

Después iniciamos con la configuración

4.1 CONFIGURACION INTERFACES

Se realiza la configuración de las interfaces de red:

Figura 20. Configuración de red

4.2 DASHBOARD

Procedemos a la verificación de las interfaces

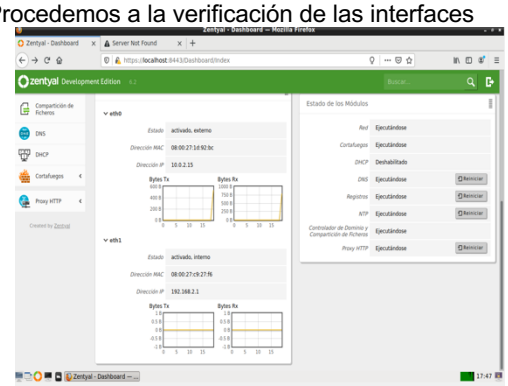

Figura 21. Estado de la configuración de red

4.3 CONFIGURACION DHCP

Realizamos la configuración de un rango de IP´s para que sean asignadas.

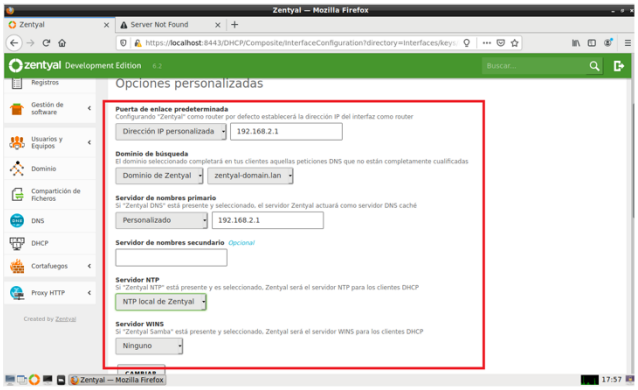

Figura 22. Configuración de un rango de IP´s

Realizamos la configuración del DNS dinámico

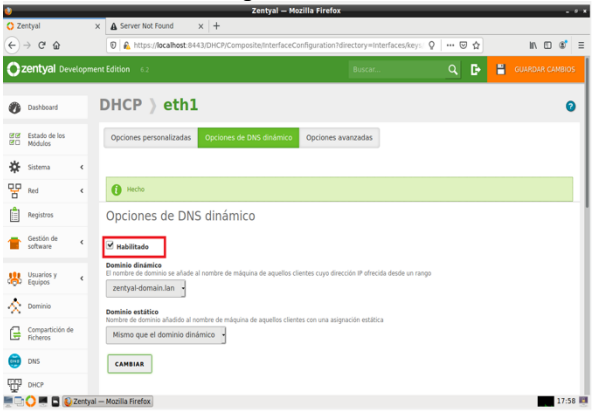

Figura 23. Habilitar DNS dinámico

4.4 COFIGURACION DESKTOP EL ADAPTADOR DE RED

En el equipo desktop realizamos las configuraciones de red interna

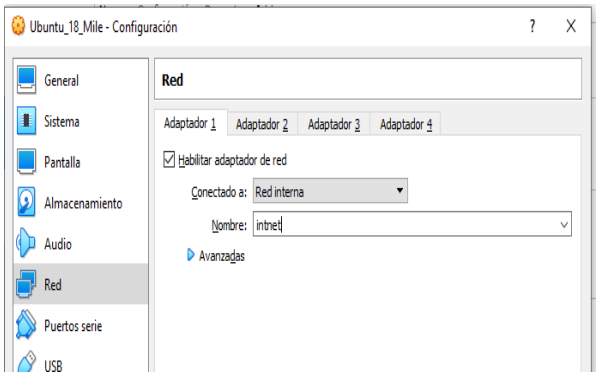

Figura 24. Configuración de red en el equipo Desktop

4.4 DETECCION IP EN DASHBOARD

Acá el servidor detecta la ip asignada

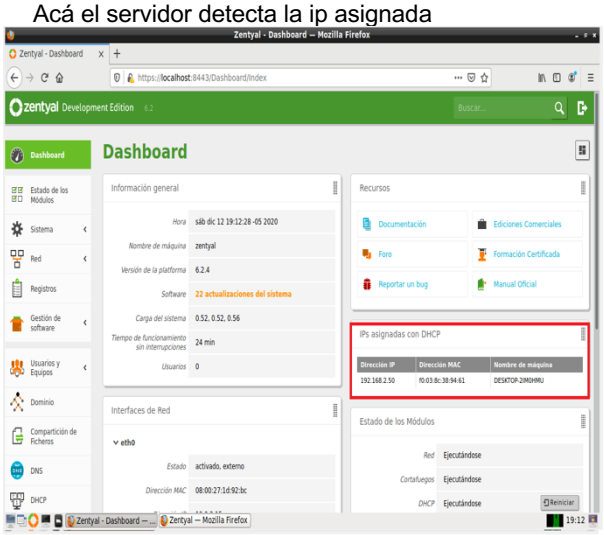

Figura 25. Servidor detecta la ip asignada

4.5 PROXY HTTP

En este paso se configurar el servicio de Proxy HTTP.

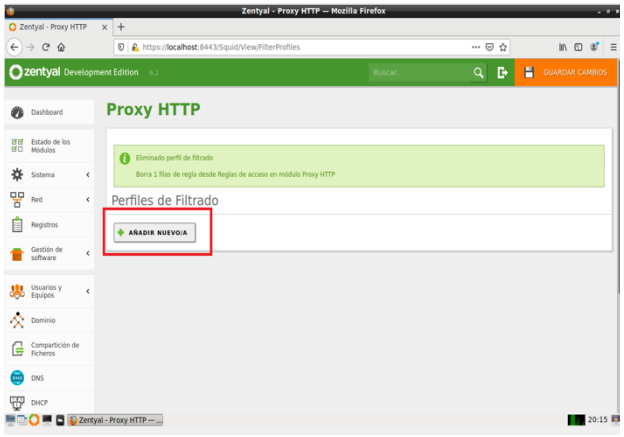

Figura 26. configurar el servicio de Proxy HTTP.

Realizamos la asignación de un nombre a nuestro perfil de filtrado

Figura 27. nombre del perfil de filtrado

4.6 CONFIGURACION

Procedemos a realizar la configuración del perfil Tiendas que fue como le coloque a ni perfil dado que la pagina que se bloqueará será una tienda multiplataforma

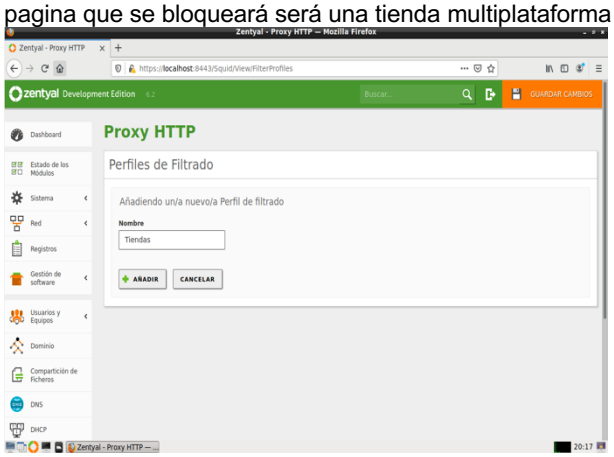

Figura 28. Configuración del perfil

Acá podemos colocar el umbral que deseamos para el perfil

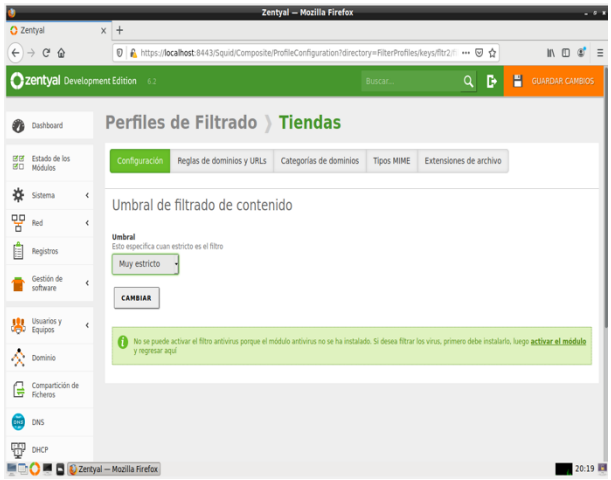

Figura 29. Umbral para el perfil

4.7 CONFIGURACION DEL FILTRADO DE DOMINIO

En este paso procedemos a colocar la URL de la cual deseamos bloquear

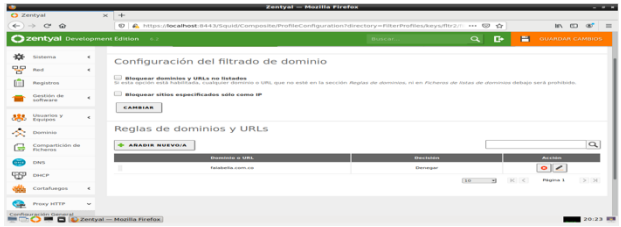

Figura 30. URL a bloquear

4.8 CONFIGURACION DE LA REGLA

En esta configuración colocamos el perfil que creamos con anterioridad al cual le colocamos el nombre TIENDAS , acá definimos como queremos realizar la definición de en que espacio de tiempo queremos aplicar la restricción.

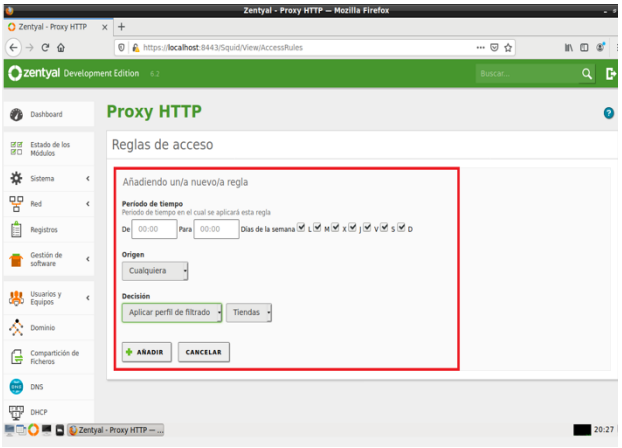

Figura 31. aplicar la restricción

4.9 CONFIGURACION PUERTO Y HABILITACION DEL PROXY

Es este paso procedemos inicialmente a la definición del puerto en nuestro caso 1230

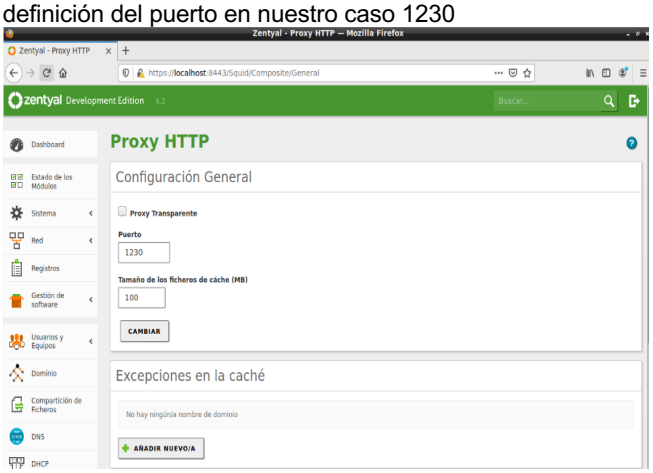

Figura 32. aplicar la restricción

Procedemos a ingresar a nuestro desktop para validar que inicialmente nos permite acceder a la página que vamos a bloquear.

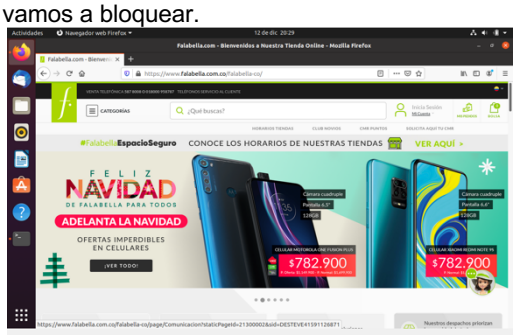

Figura 33. acceder a la página que vamos a bloquear

Realizamos la activación del proxy

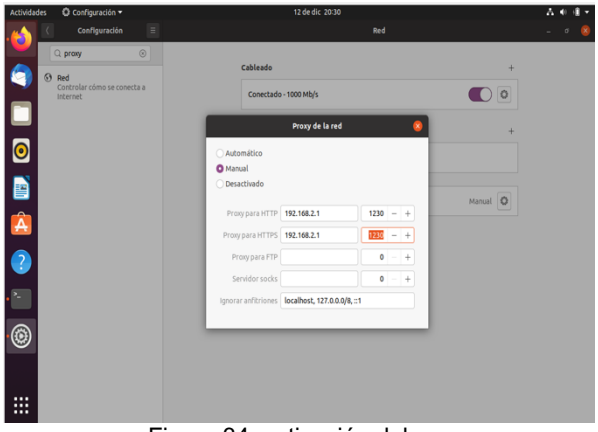

Figura 34. activación del proxy

4.10 CONFIGURACION DEL PROXY

Procedemos con la configuración del proxy y con esto procedemos a realizar las pruebas para validar que efectivamente no nos permite el acceso a la pagina restringida, pero si podemos acceder a otras páginas

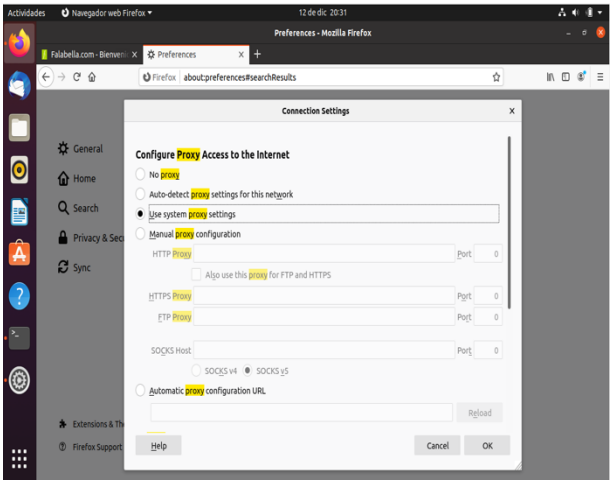

Figura 35. acceso a la pagina restringida

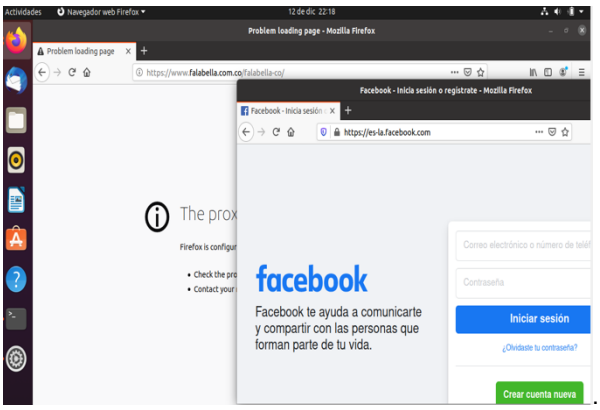

Figura 36. acceso a la pagina restringida

5 CORTAFUEGOS

Una vez la configuración del DHCP y DNS han sido realizadas y comprobadas, con el fin de establecer políticas en el cortafuegos es necesario realizar su instalación, para en la configuración inicial del Zentyal puede realizarse su instalación, o en caso contrario desde Gestión de Software.

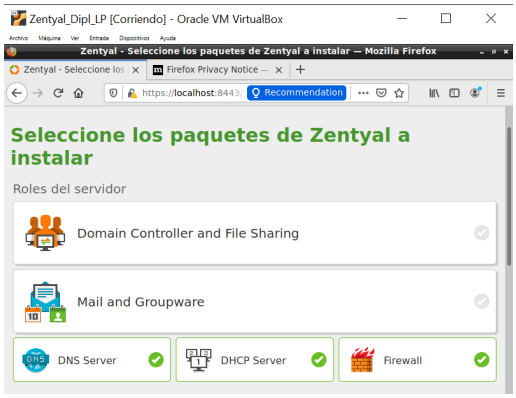

Figura 37. Instalación componente Firewall

Con el componente instalado, la configuración consiste en la creación de un servicio, un objeto y las reglas correspondientes.

5.1 CREACIÓN DE SERVICIO

Un servicio permite delimitar a nivel de protocolo y puerto los elementos que serán tratados, para el caso particular se crea uno cuyo propósito sea analizar el tráfico TCP/UDP bajo los puertos 80 y 443, correspondientes a los servicios Web, para esto desde el menú *Red* bajo *Servicios* se crea este:

Figura 38. Creación de servicio

Una vez ha sido creado se agregan los dos elementos mencionados correspondientes al protocolo y puertos:

Figura 39. Adición de servicio

5.2 CREACIÓN DE OBJETO

El objeto nos va a permitir reconocer a quién se va a gestionar en el cortafuegos, en este caso se creará uno donde se defina el rango de IP usadas por Twitter que será el sitio que será bloqueado, pruebas realizadas indican que esta página responde a la red 104.244.42.x, por lo que el objeto tendrá como característica este rango de IP:

Figura 40. Objeto a gestionar

5.3 CREACIÓN DE REGLA

Puesto que, por medio del servicio se reconoce qué se va a gestionar, y con el objeto a quién se gestionará, la regla nos permite determinar qué se va a realizar entre estos dos elementos, para ello se debe reconocer los siguientes elementos:

Decisión: Indica qué se realizará con los paquetes que cumplan las características de la regla, las opciones son: Permitir, Denegar o Registrar. En el caso actual se usará Denegar puesto que se pretende el bloqueo de conexiones.

Origen: Determinar desde qué punto origen se ejecutará la operación por parte del cortafuegos, se puede determinar una IP en particular o un objeto, para esta actividad se dejará como Cualquiera, de esta forma cualquier origen ejecutará la regla.

Destino: Determina a qué punto final va dirigida la comunicación, en este caso se hará uso del objeto previamente creado para que tenga en cuenta las IP relacionadas a Twitter.

Servicio: Cuando la regla se aplica, determina a qué protocolo/puerto aplicará, y se usará el servicio creado previamente.

Descripción: Indicación breve sobre el contenido de la regla para propósitos de reconocimiento.

Con esta configuración la regla tendrá estas características:

Figura 41: Regla creada

5.4 RESULTADOS CORTAFUEGOS

Una vez se han configurado y guardado estos parámetros, al momento de ejecutar una conexión vía web se obtendrá un *timed out* en el explorador web, que nos indica que la regla ha sido ejecutada e impide la conexión:

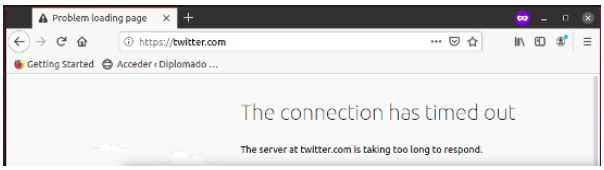

Figura 42: Respuesta explorador Web

Ahora, puesto que la regla ha sido creada con el servicio que tiene en cuenta protocolo TCP/UDP bajo puertos 80 y 443, la respuesta de ping no será afectada:

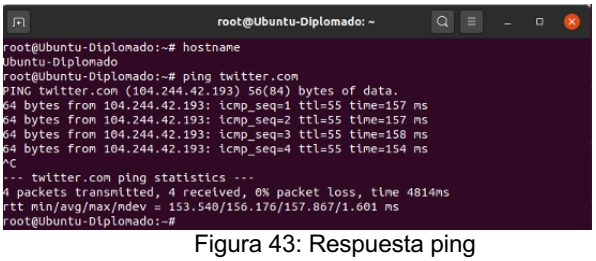

Figura 43: Respuesta ping

6 FILE SERVER, PRINT SERVER

El file server permite compartir carpetas y estas a su vez archivos entre maquinas Ubuntu, en su grupo de trabajo, el cual se configura desde Zentyal.
Se crea la unidad organizativa.

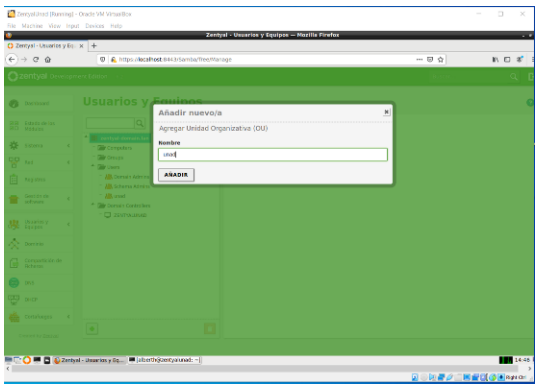

Figura 44. Unidad organizativa

Creamos un grupo para los usuarios que se necesitan crear.

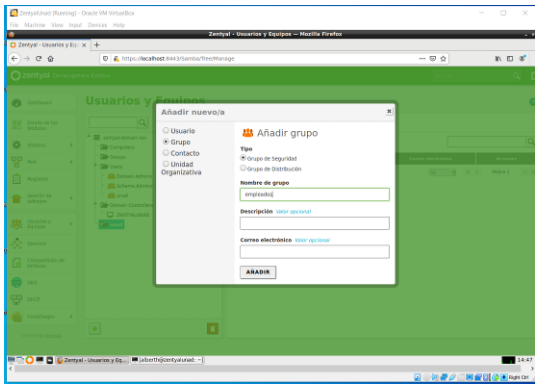

Figura 45. Grupo empleados

Añadimos el usuario que vamos a administrar.

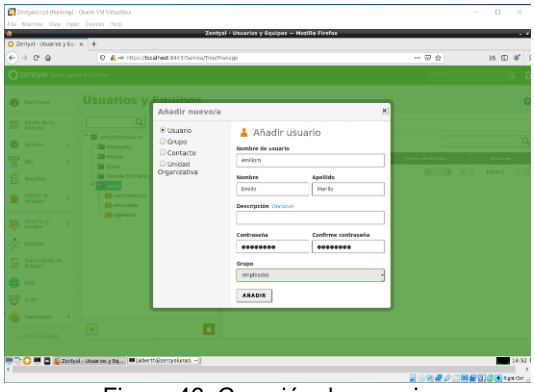

Figura 46. Creación de usuario

Vinculamos Ubuntu a Zentyal para tener poder compartir la carpeta.

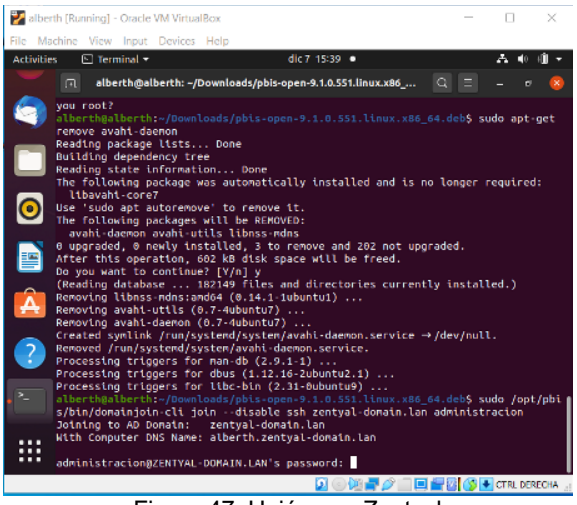

Figura 47. Unión con Zentyal

En este apartado compartimos los ficheros para el usuario previamente creado.

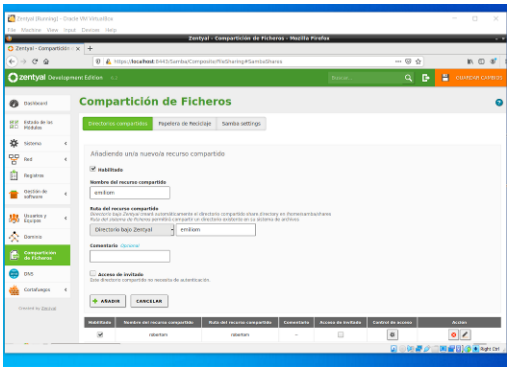

Figura 48. Compartir ficheros

En Zentyal para que una configuración surta efecto es necesario siempre guardar cada paso que se realiza.

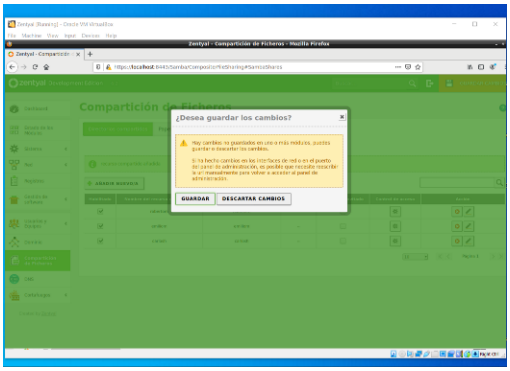

Figura 49. Guardamos la configuración

En esta sección se habilitan los permisos que para este caso daremos de lectura y escritura.

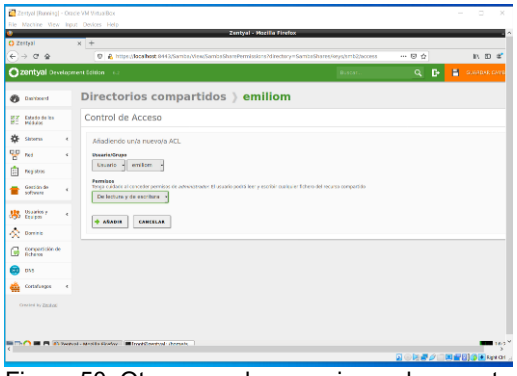

Figura 50. Otorgamos los permisos a la carpeta

Verificamos los permisos desde ubuntu

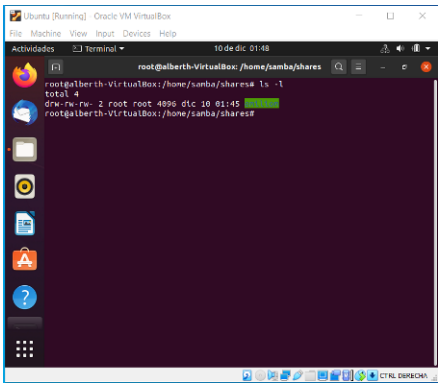

Figura 51. Verificamos los permisos de la carpeta

7 VPN

Procedemos con la implementación y configuración de una Red Privada Virtual, para ello instalamos los servicios de VPN y Certification Authority; esto por el modulo de Gestión de Software. Ingresando por el servicio de Certification Authority creamos un primer certificado para nuestro Zentyal.

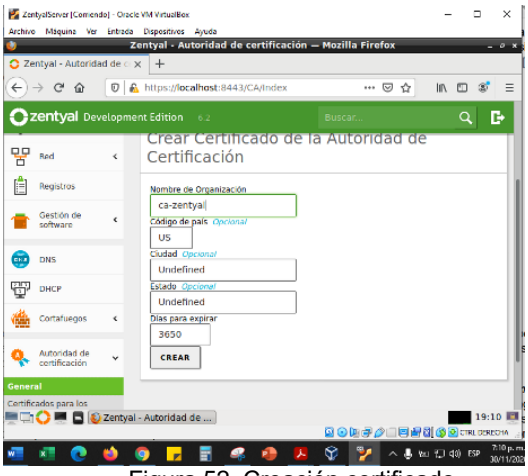

Figura 52. Creación certificado

Procedemos a crear nuestro servidor VPN, ingresando por VPN, Servidores.

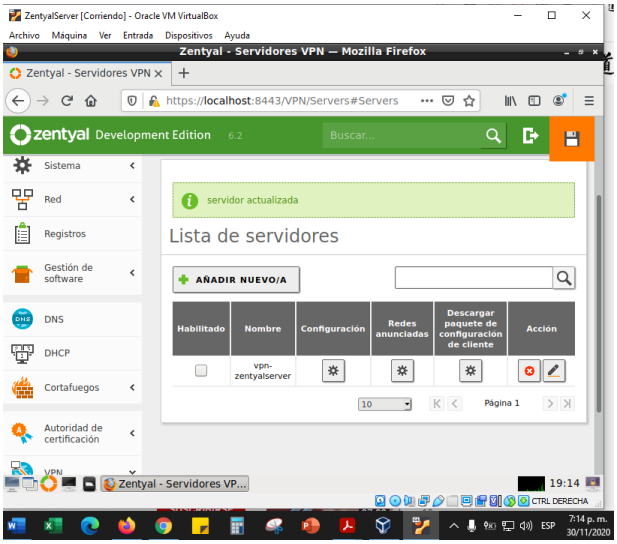

Figura 53. Creación servidor VPN

Se debe configurar, se selecciona la opción interfaz TUN y los demás espacion pueden quedar por defecto.

Nuevamente por la opción Autoridad de certificación, creamos el certificado para nuestro cliente.

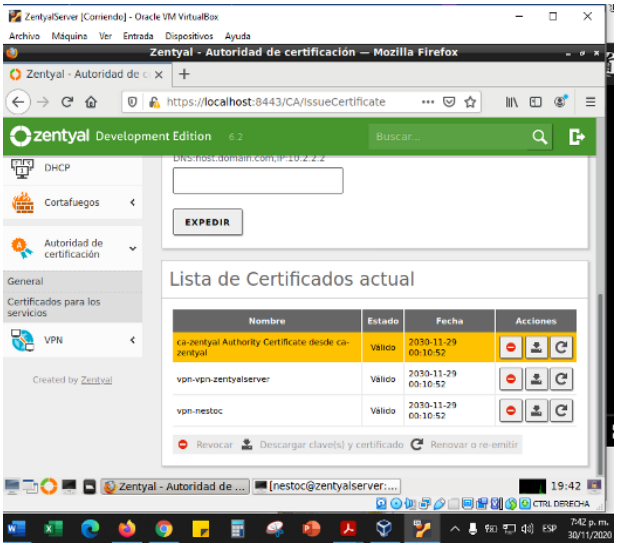

Figura 54. Observamos los certificados creados

A continuación, descargamos el certificado del cliente y en el espacio tipo cliente indicamos el sistema operativo donde será ejecutado, certificado del cliente seleccionamos el certificado creado, en dirección del servidor indicamos la IP de nuestro servidor Zentyal.

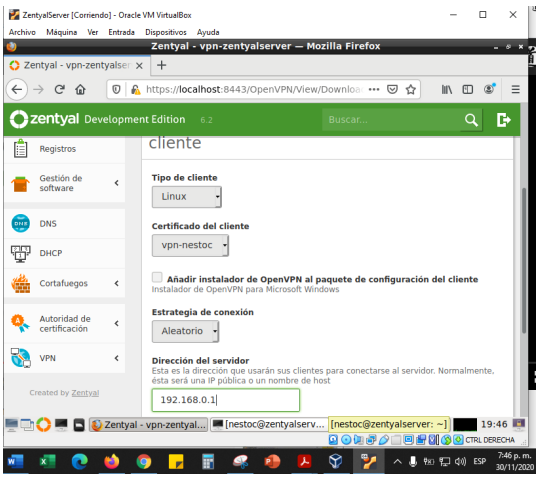

Figura 55. Descarga certificado cliente

Por la opción de Red, Servicios, añadimos el nuevo servicio VPN y configuramos el puerto de entrada (destino) que de forma predeterminada es el 1194

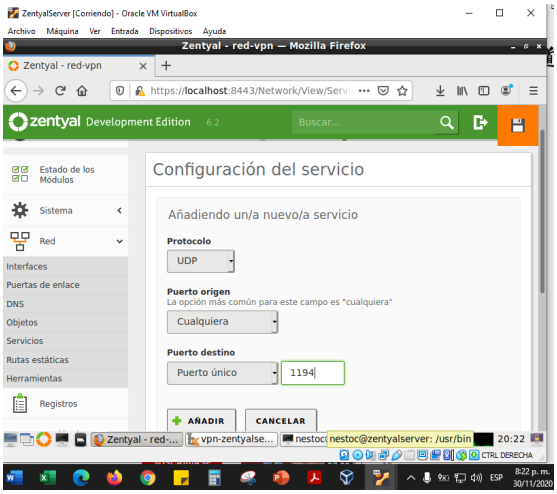

Figura 56. Configuración del servicio

En el cortafuegos es necesario configurar la opción de filtrado, para ello creamos una nueva regla de conexión

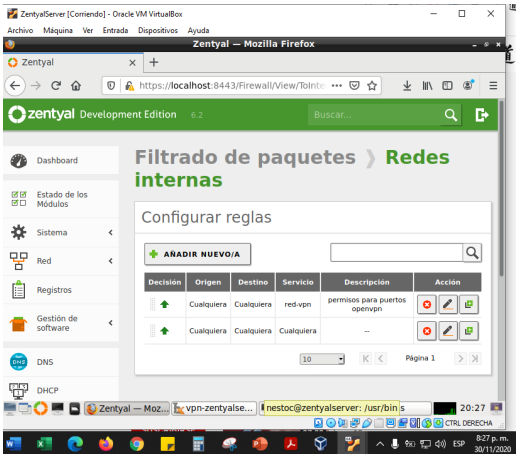

Figura 57. Regla creada y configurada

En el dashboard de Zentyal corroboramos que el servicio VPN este creado, configurado y activo.

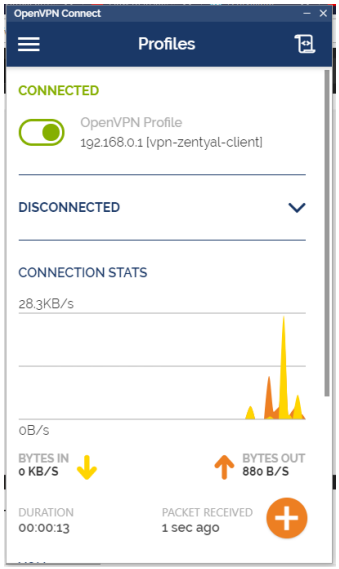

Figura 58. Verificamos conexión en W-10

En el desktop Ubuntu activamos la VPN de forma automática por la opción de Red, cargando el archivo descargado y transferido a dicha maquina

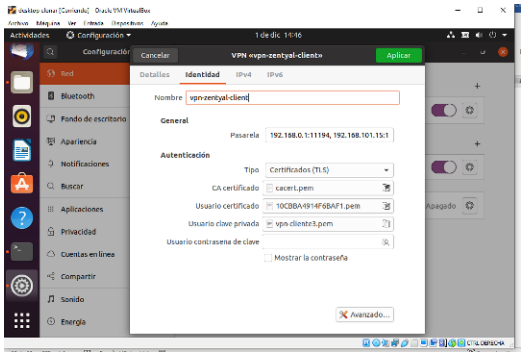

Figura 59. Vista activación VPN en desktop Ubuntu

En desktop Ubuntu hacemos un ifconfig para verificar el otorgamiento de dirección IP y la VPN activa

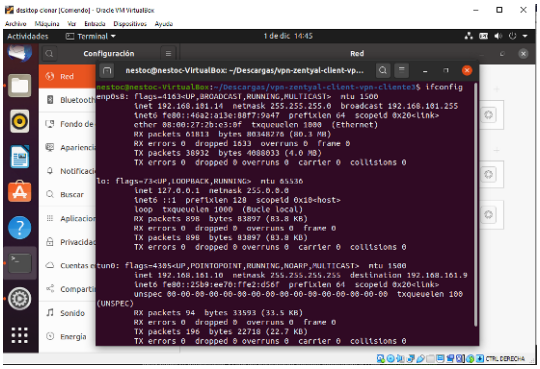

Figura 60. IP enp0s8 y tun0

En la siguiente imagen observamos la VPN activa en el desktop Ubuntu, el recuadro corresponde a la esquina superior derecha de la figura 42.

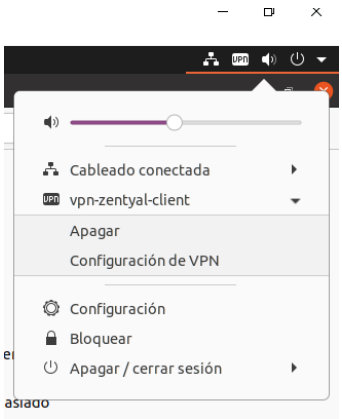

Figura 61. VPN activa en desktop Ubuntu

Procedemos a efectuar conexión desde desktop Ubuntu y observamos el acceso a Zentyal Server, desde el mismo servidor y desde el desktop, esto a través de la VPN.

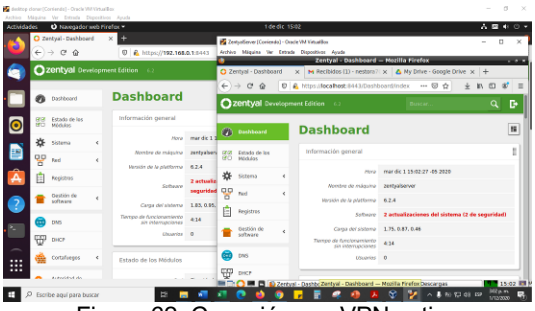

Figura 62. Conexión por VPN activa

8 CONCLUSIONES

Al gestionar Zentyal se demuestra el funcionamiento con los servicios de red protegida por el firewall Endian. Los clientes de la red se enlazan al dominio local a través del servidor DNS que resuelve las solicitudes almacenándola en chache por cada petición durante un período de tiempo determinado reduciendo el tiempo de cada la conexión de red y el consumo de tráfico hacia Internet.

El servidor DHCP conectar los dispositivos con una asignación automática de direcciones de red, al solicitar la configuración IP el servidor recurre a una base de datos que contiene los parámetros de red asignables con los rangos de direcciones IP disponibles para ser concedidos en la interfaz de red.

Por medio de la configuración de elementos como Servicios y Objetos, la gestión de las reglas del cortafuegos permite una administración organizada y centralizada, evitando crear reglas repetitivas sobre elementos individuales ya que se pueden agrupar. Por

otra parte, se debe tener sumo cuidado con cada uno de los parámetros de las reglas en el cortafuegos, con el fin de evitar el bloqueo a servicios que deben encontrarse abiertos y pueden afectar directamente la operación de la compañía.

Es evidente el avance que presentan las distribuciones Linux, el trabajo de desarrolladores y programadores brindan a los usuarios alternativas de fácil manejo con herramientas muy completas para desarrollar labores de escritorio o de servidor, como en este caso con la distribución Zentyal; la cual cuenta con una amplia documentación que permite fácilmente su configuración.

9 REFERENCIAS

[1] Zentyal (2004). *Alternativa Linux Fácil a Windows Server*. [En línea]. Disponible en: http://www.zentyal.com/es/

[2] Zentyal S.L. (2004). *Documentación de Zentyal 6.2* [En línea] Disponible de: https://doc.zentyal.org/es/index.html

[3] JGAITPRO. (2014). *Zentyal - Instalar y configurar DHCP Server*. [En línea]. Disponible en: https://youtu.be/H5lhAKOH5LM

[4] JGAITPRO. (2014). *Zentyal - Instalar y configurar DNS Server*. [En línea]. Disponible en: https://youtu.be/bmROdq3pRmc

[5] ZENTYAL. *Cortafuegos*. [En línea]. Disponible en: https://doc.zentyal.org/es/firewall.html

[6] Zentyal 6.2 Official Documentation — Zentyal 6.2 Documentation. (2020). Retrieved 1 December 2020, from https://doc.zentyal.org/en/

[7] (2020). Retrieved 1 December 2020, from https://www.youtube.com/watch?v=8zaxU1C7qBc

[8] Cómo configurar una VPN PPTP en Ubuntu. (2012). Retrieved 1 December 2020, from https://www.xatakamovil.com/conectividad/como-configurar-una-vpn-pptp-en-ubuntu

[9] How To Set Up and Configure an OpenVPN Server on Ubuntu 20.04 | DigitalOcean. (2020). Retrieved 1 December 2020, from https://www.digitalocean.com/community/tutorials/how-to-set-up-and-configure-an-openvpn-server-on-ubuntu-20-04

[10] (2020). Retrieved 1 December 2020, from https://www.youtube.com/watch?v=3rNfipxE-9o