SOLUCIONANDO NECESIDADES ESPECÍFICAS CON GNU/LINUX.

Álvaro Galvis
agalvisga@unadvirtual.edu.co
Jeisson Lenis
jlenism@unadvirtual.edu.co
Jesús David Bernal Mejía
jbernalme@unadvirtual.edu.co
Manuel Felipe Montoya Porras
mfmontoyap@unadvirtual.edu.co
Vanessa Vargas Mariño
vvargasm@unadvirtual.edu.co

RESUMEN: *En el presente informe, estudiaremos la implementación de un servidor bajo el sistema operativo GNU/Linux en su distribución Zentyal versión 5.0, el cual permitirá a los administradores de servicios tecnológicos e informáticos de una compañía o persona independiente de administrar servicios de redes (como VPN, DHCP, DNS y controlador de dominio), administración de bases de datos (como MySQL o PostgreSQL, entre otros), administración de servicios WEB (como hosting, pagos en línea, blogs y WEB sites entre otros), seguridad informática (administración de firewall, proxy y administración de puertos) y por ultimo administración de archivos y carpetas (file server y print server, etc.). De manera que el administrador pueda de forma intuitiva configurar correctamente los servicios que se requieran y dar un mantenimiento tanto preventivo como correctivo de la infraestructura tecnológica que administra.*
Se demostrará la instalación y funcionamiento de esta distribución y garantizaremos su correcto funcionamiento bajo los requerimientos exigidos para una infraestructura determinada y así garantizar una seguridad informática y buenas prácticas del manejo de la tecnología.

PALABRAS CLAVE: Seguridad Informática, Servicios de red, Servicios WEB, Zentyal 5.0.

1 INTRODUCCIÓN

Actualmente la dinámica de la administración de la información y su seguridad, son compromisos de alto valor y responsabilidad en las empresas he incluso para personas independientes que a diario recuren a una minería de datos para ya sea por trabajo, comunicación e incluso el ocio. Día a día la información crece y con ella su nivel de seguridad, dado a que entre más información exista sobre una persona, mejor es la forma de diagnosticar sus necesidades, conocer más sobre un lugar e incluso las estrategias empresariales de una compañía.

Debido a ello se han ido desarrollando soluciones tecnológicas para la correcta administración de la información y con ello garantizar la seguridad informática bajo una serie de servicios que se prestan para los usuarios, estas soluciones se basan principalmente de las necesidades de una compañía la cual, para garantizar sus servicios, adquiere un ordenador de tipo servidor, el cual en este caso busca implementar servicios de red como DHCP Server, DNS Server, VPN y Controlador de Dominio; Proxy no transparente y contrafuegos para la administración de seguridad informática, y por ultimo administración de archivos e impresora; todo bajo una infraestructura de red de una red WAN, LAN y DMZ.

2 INSTALACIÓN ZENTYAL

2.1 CARACTERÍSTICAS GENERALES

Nos dirigimos a la página principal de zentyal https://zentyal.com/community/ y en la parte inferior de la página WEB podremos encontrar las diferentes versiones del sistema operativo, para el caso se descargará la versión 5.0.

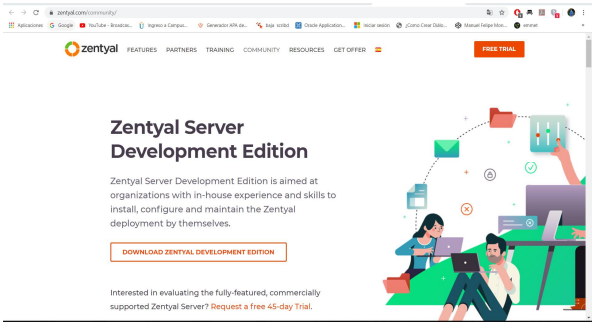

Imagen 1. Página WEB principal de Zentyal

Se realizan los ajustes recomendamos por el proveedor del servidor Zentyal para la configuración de la máquina virtual como, memoria RAM, tamaño de disco duro virtual, interfaces de red que en este caso serán 2, una WAN y una LAN administradas por el servidor Zentyal, también se debe de montar en el dispositivo virtual de CD el archivo .ISO anteriormente descargado e iniciar la máquina virtual.

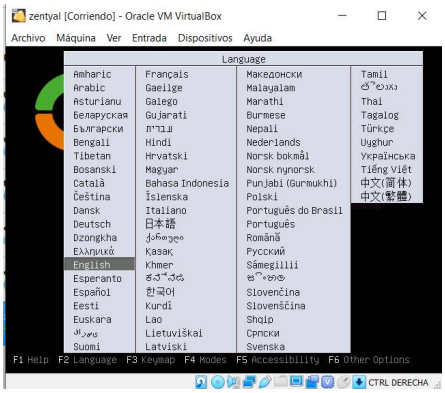

Imagen 2. Inicio de Zential

Seleccionamos el idioma principal y luego iniciamos la instalación del servidor, luego nos preguntara por la ubicación del servidor, la distribución del teclado, el nombre del servidor, el usuario y contraseña del administrador y cuál es la interfaz de red principal del servidor dado a que se administraran 2, para este caso será la WAN.

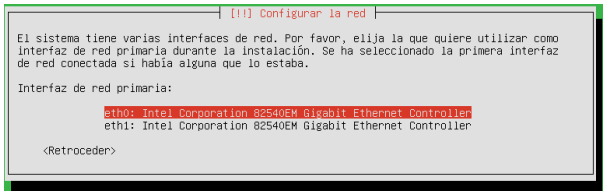

Imagen 3. Selección de interfaz de red principal

La instalación continuará de forma automática realizando actualizaciones correspondientes hasta finalizar, luego de ello nos pedirá reiniciar la máquina.

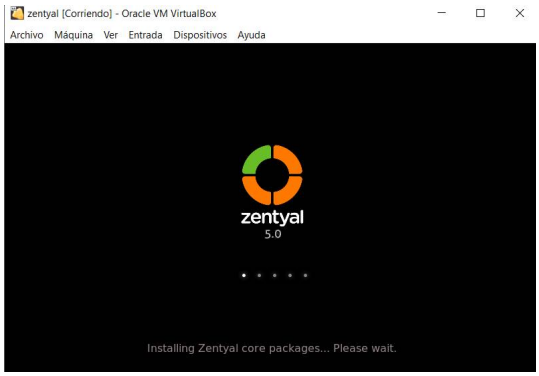

Imagen 4. Inicio principal de Zentyal.

Al iniciar la máquina, esta solicitará el usuario y contraseña anteriormente parametrizados en la instalación, luego de ello se abrirá el escritorio de la distribución del sistema operativo y a continuación, se abrirá el navegador WEB con la página principal del administrador (localhost) del servidor.

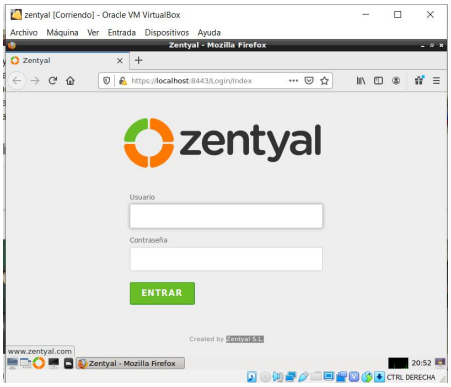

Imagen 5. Interfaz de inicio del servidor Zentyal 5.0.

Nuevamente ingresamos el mismo usuario y contraseña anteriormente parametrizada e ingresamos, a continuación, nos pedirán que seleccionemos los servicios que vallamos a utilizar en nuestro servidor.

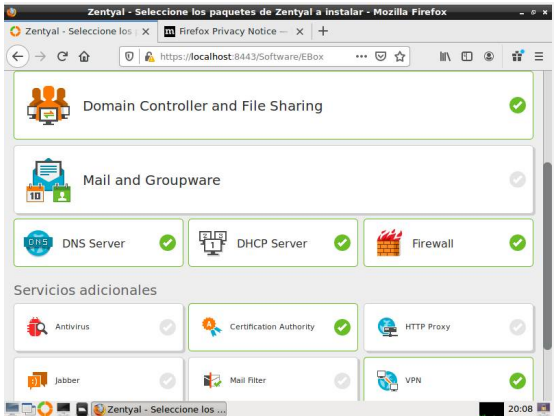

Imagen 6. Selección de servicios en Zentyal 5.0.

Después de ello, se asignará las direcciones IP para los entornos WAN y LAN respectivamente, en este caso la WAN tomará una IP que asigne nuestro IPS (proveedor de servicios internet) y la LAN una dirección que se halla calculado para la configuración determinada de un numero de máquinas que estarán en esta red, y de esta forma se concluye la instalación inicial del servidor Zentyal 5.0.

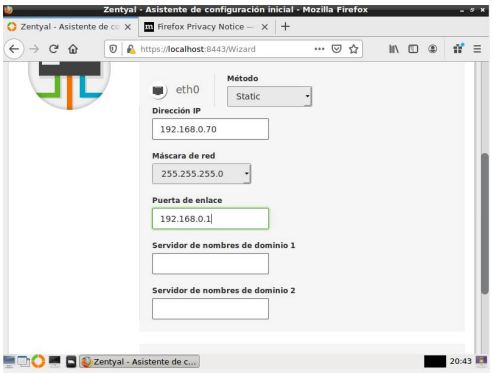

Imagen 7. Configuración de interfaces de red.

3 ACTIVIDADES A DESARROLLAR

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

Producto esperado: Implementación y configuración detallada del acceso de una estación de trabajo GNU/Linux Ubuntu Desktop a través de un usuario y contraseña, así como también el registro de dicha estación en los servicios de Infraestructura IT de Zentyal.

Lo primero que debemos hacer es verificar el estado de los módulos y activar el Controlador de Dominio, el DNS y DHCP. Luego vamos a ingresar un nombre para la máquina y el dominio.

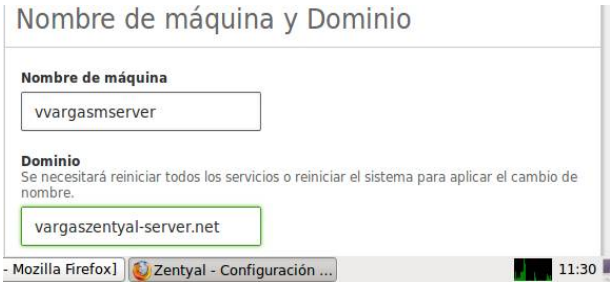

Imagen 8. Configuración del dominio.

Procedemos a revisar el Dashboard, en el cual se podrá verificar el estado activo de las dos interfaces de red que se configuraron con anterioridad.

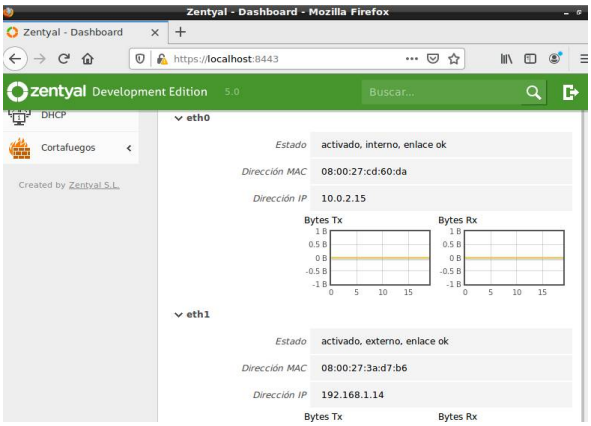

Imagen 9. Estado de las interfaces de red.

Configuramos los rangos de red de IP, pero antes debimos los rangos que tenemos disponibles, en mi caso iban de 192.168.1.1 al 192.168.1.254.

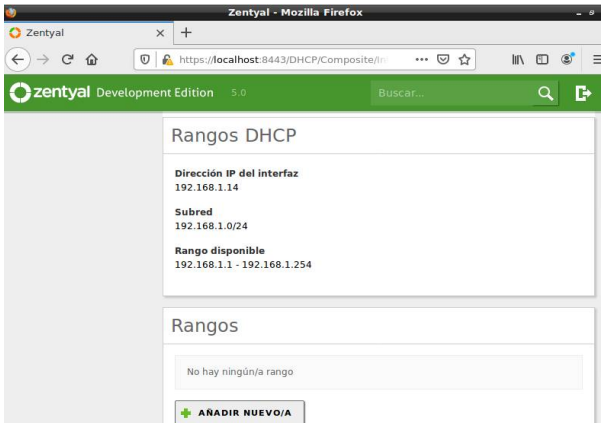

Imagen 10. Verificación de rangos disponibles.

Configuramos la red local en el rango 192.168.1.120 a 192.168.1.150.

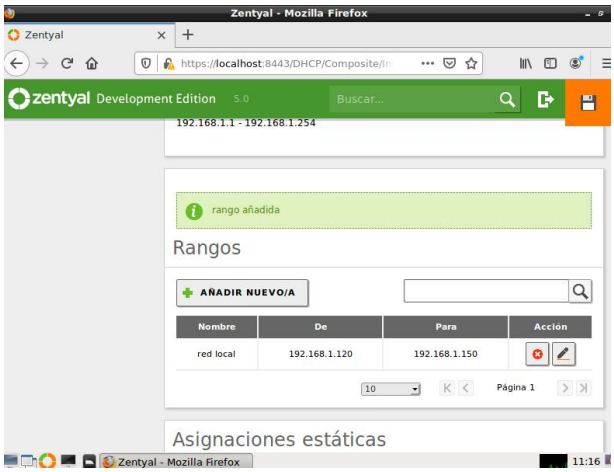

Imagen 11. Configuración del rango de red local.

Ahora vamos a validar el nombre de nuestro dominio.

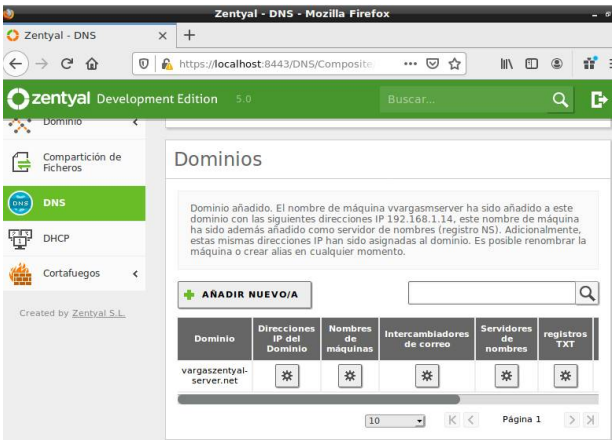

Imagen 12. Validación del nombre del dominio.

Debemos crear un grupo al cual llamaremos tematica1 y también crearemos un usuario llamado vanessa, luego se procede a añadir el usuario "vanessa" al grupo "tematica1".

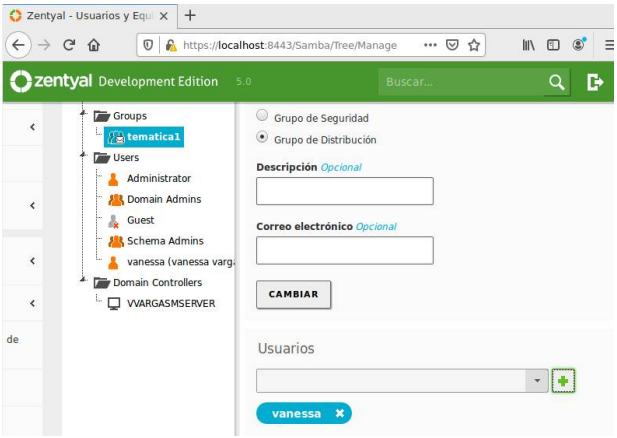

Imagen 13. Asignación de usuario al grupo tematica1.

Ahora nos dirigimos a Ubuntu desktop y actualizamos el sistema con el comando: sudo apt-get update.

Luego vamos a instalar Keberos KDC con el siguiente comando: sudo apt-get install krb5-kdc krb5-admin-server krb5-config, una vez hecho esto nos va a aparecer en la pantalla dos preguntas, la primera es para configurar el nombre de reino que se configuró en el dominio de Zentyal, y la segunda es el nombre del servidor. Una vez se ha terminado con este paso lo que se hace es validar la IP que tenemos con el comando: ifconfig, ahora solo ejecutamos el comando route para validar la tabla de rutas IP del núcleo. Luego en el fichero /etc/network/interfaces veremos asegurada la IP estática.

3.2 TEMÁTICA 2: PROXY NO TRANSPARENTE

Producto esperado: Implementación y configuración detallada del control del acceso de una estación GNU/Linux Ubuntu Desktop a los servicios de conectividad a Internet desde Zentyal a través de un proxy que filtra la salida por medio del puerto 3128.

Para esto debemos instalar el componente "HTTP Proxy", para ello vamos al panel de la izquierda, Software » Componentes de Zentyal y allí veremos la lista de componentes disponibles.

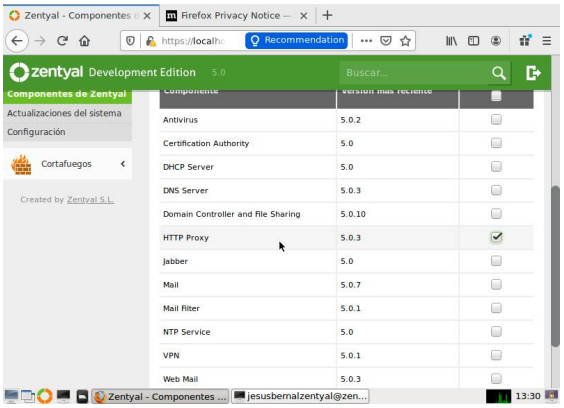

Imagen 14. Identificación del componente

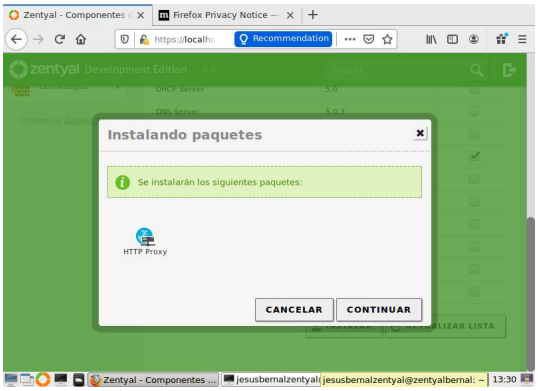

Imagen 15. Instalación HTTP Proxy

Por defecto este componente queda desactivado, debemos ir “Estado de módulos” y activarlo para poder usarlo.

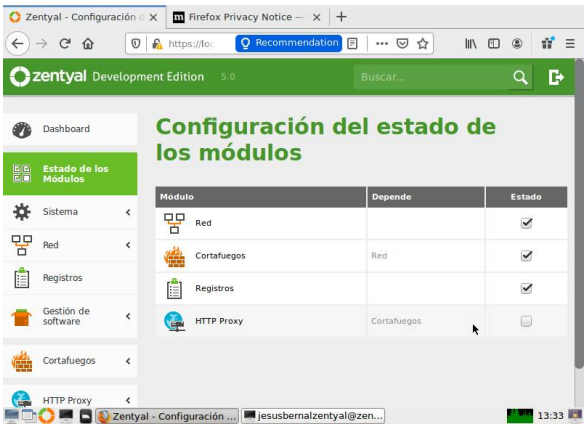

Imagen 16. Estado del componente

Nos dirigimos al componente que acabamos de instalar “HTTP Proxy” e ingresamos en “General Settings”, allí dejamos sin marcas la opción de proxy transparente y el puerto lo dejamos en 3128 como lo pide la guía.

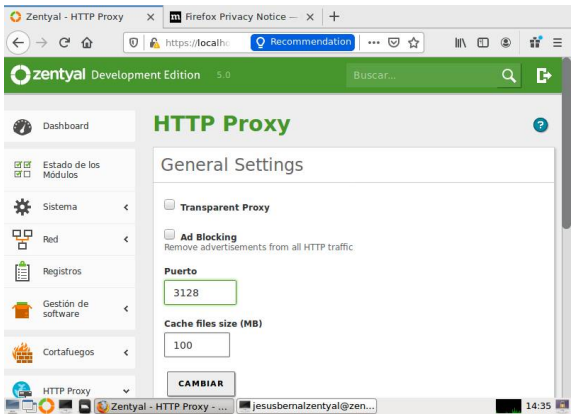

Imagen 17. Configuración de HTTP Proxy

Creamos un perfil nuevo de filtrado en “Filter Profile” y lo configuramos.

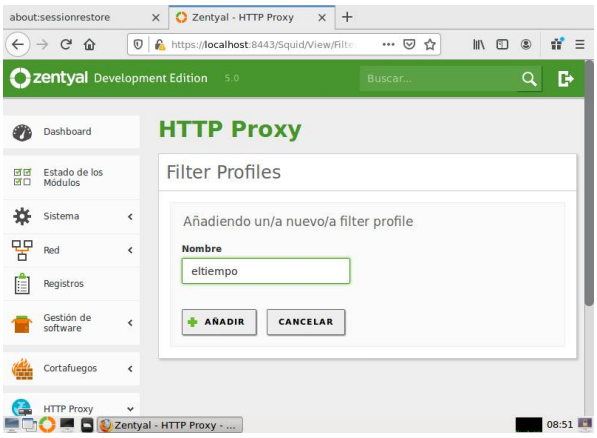

Imagen 18. Creación perfil de filtrado

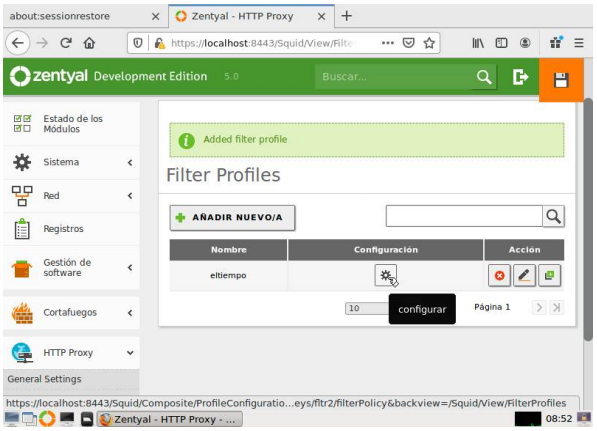

Imagen 19. Configuración del perfil de filtrado

Allí podremos ajustar que tan estricto será este perfil y en la pestaña “Domains and URLs” configurar que paginas serán permitidas o bloqueadas, en mi caso bloquearé el tráfico a eltiempo.com.

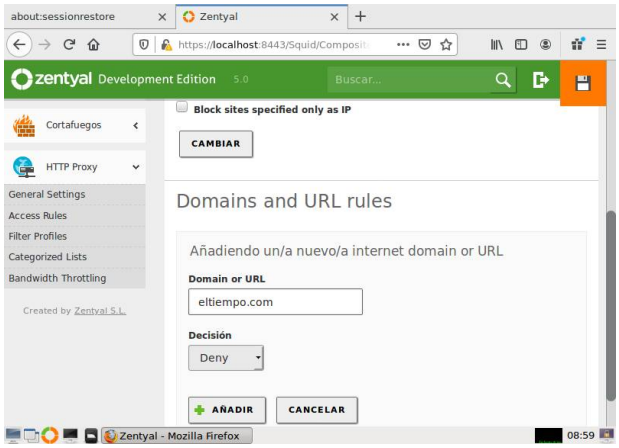

Imagen 20. Dominio a bloquear

Vamos a “Access rules” donde por defecto hay una regla que permite todo el tráfico, para cualquiera a través del proxy.

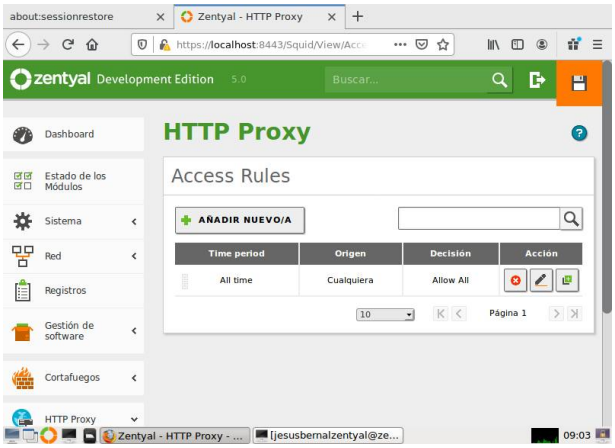

Imagen 21. Reglas de HTTP Proxy

Procedemos a editar dicha regla y le añadimos en la opción “Decisión” el perfil de filtrado anterior.

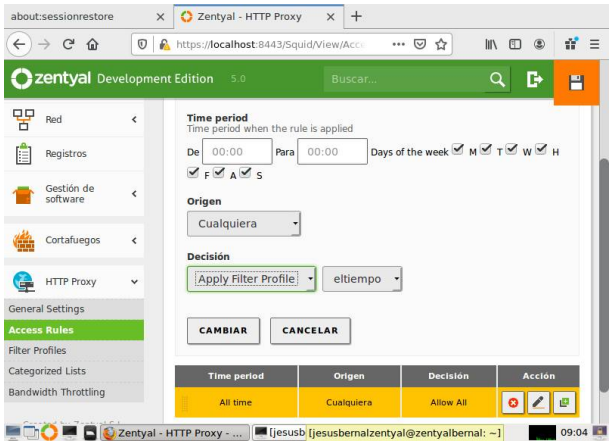

Imagen 22. Configuración de regla

Damos en cambiar y en la parte superior derecha donde está el icono de un diskette, para aplicar todos los cambios que realizamos.

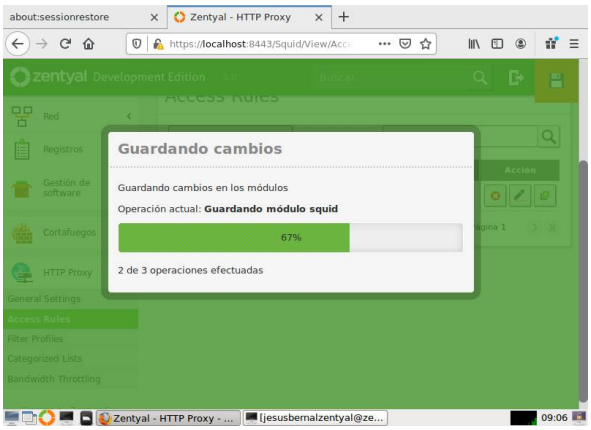

Imagen 23. Guardando cambios

Ahora identificamos la IP que tiene la segunda interfaz de red, en este caso es 192.168.1.106.

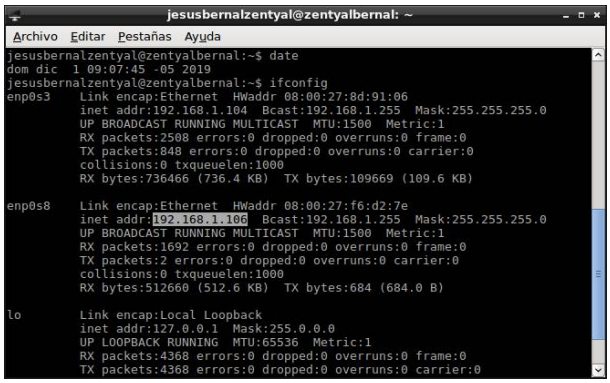

Imagen 24. IP interfaz interna

Iniciamos nuestra otra máquina virtual con Ubuntu Desktop y realizamos la configuración y verificación de funcionamiento del proxy.

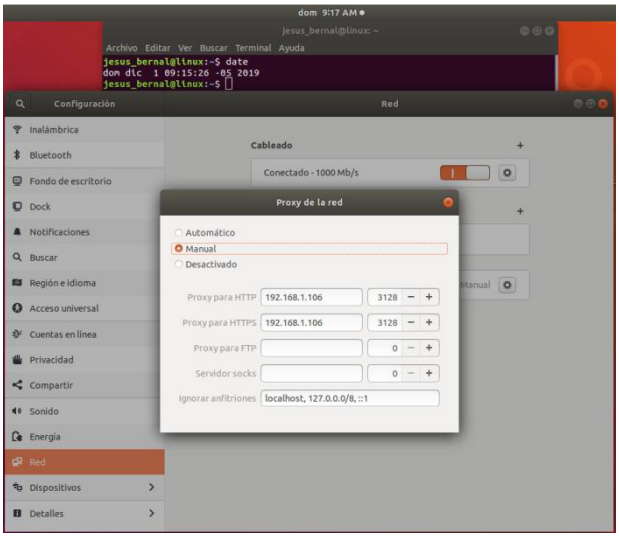

Imagen 25. Configuración del Proxy

Se evidencia el bloqueo con el proxy por el puerto 3128 de la página eltiempo.com y se observa otras como youtube.com las cuales si se logra la conexión.

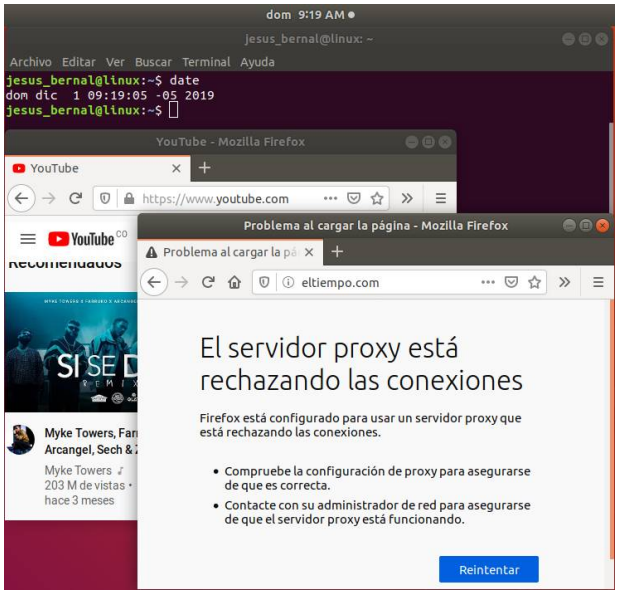

Imagen 26. Evidencia del funcionamiento

3.3 TEMÁTICA 3: CORTAFUEGOS

Se crea un objeto llamado Facebook para añadir rangos de IP's o las IP's específicas.

Imagen 27. Lista de objetos.

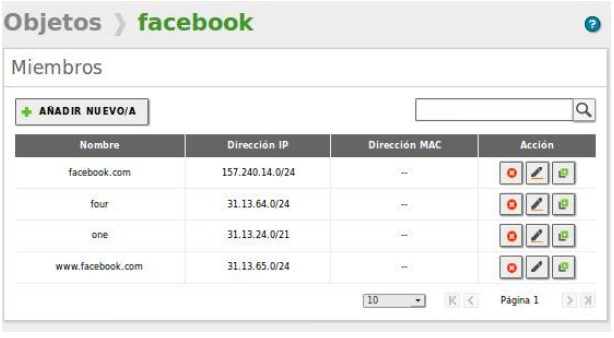

Imagen 28. Miembros de la lista

Luego en el apartado de Filtrado de Redes Internas procede la adición de los mismos, se compone de una serie opciones las cuales limitan el acceso dado su elección.

Imagen 29. Redes Internas

Configura la red de la maquina Ubuntu desktop como red interna.

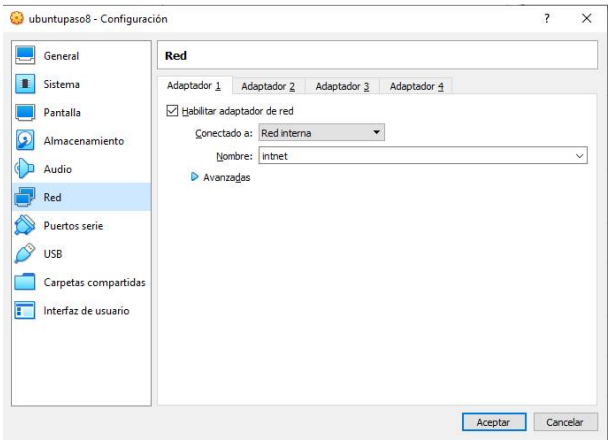

Imagen 30. Configuración de red.

Se deja por defecto la red como DHCP automático.

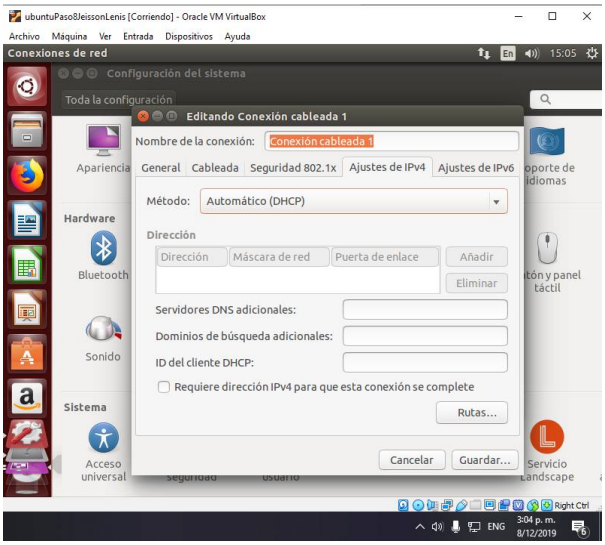

Imagen 31. Automático (DHCP)

Se comprueba mediante ifconfig cuál es la IP, efectivamente entra en el rango 20-30.

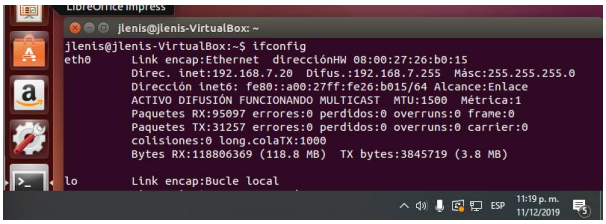

Imagen 32. Identificación de IP

La conexión caduca en el bloqueo de la misma, cabe recalcar que Facebook maneja una serie de IP las cuales a no ser que se bloqueen todas no será 100% efectiva la bloqueada de la misma.

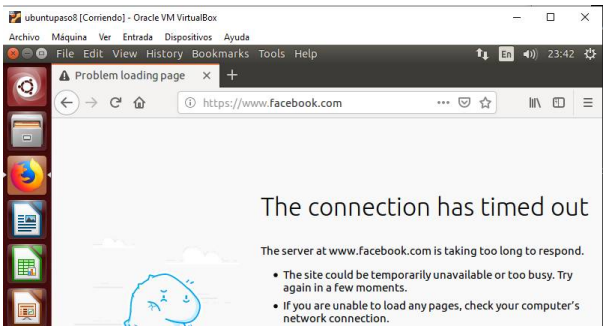

Imagen 33. Evidencia conexión fallida.

3.4 TEMÁTICA 4: FILE SERVER Y PRINT SERVER

Producto esperado: compartición de archivos e impresoras entre el servidor Zentyal y una estación de Ubuntu.

Para ello haremos diferentes configuraciones en el servidor desde agregar direcciones IP, crear usuarios con roles administrativos y permisos para conexión entre los equipos al igual que permisos para crear archivos.

Imagen 34. Selección de servicios

Seleccionamos domain controller and file sharing para su instalación.

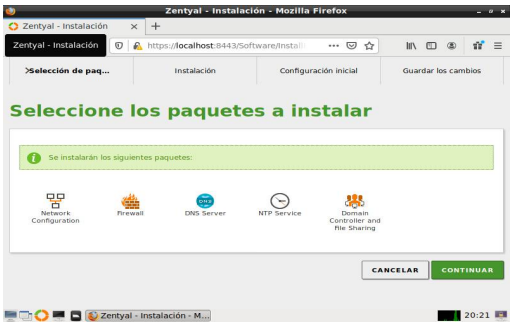

Imagen 35. Validación de servicios seleccionados

Nos muestra los paquetes que se instalaran.

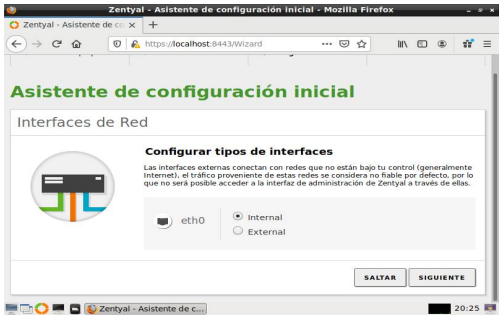

Imagen 36. Configuración de interfaz de red Configuramos interfaces de red interna.

Imagen 37. Selección de tipo de servidor

Seleccionamos el tipo de servidor lo dejamos por defecto.

Imagen 38. Finalización de instalación

Confirmación de instalación exitosa.

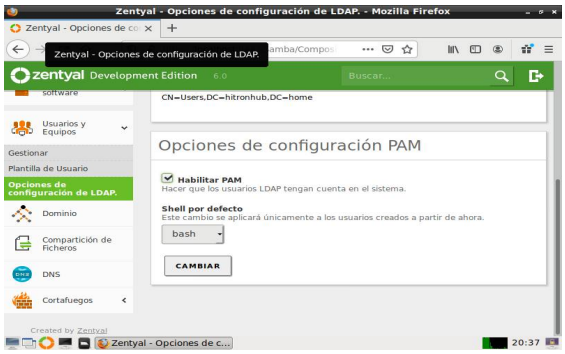

Imagen 39. Configuración PAM

Habilitamos la configuración PAM.

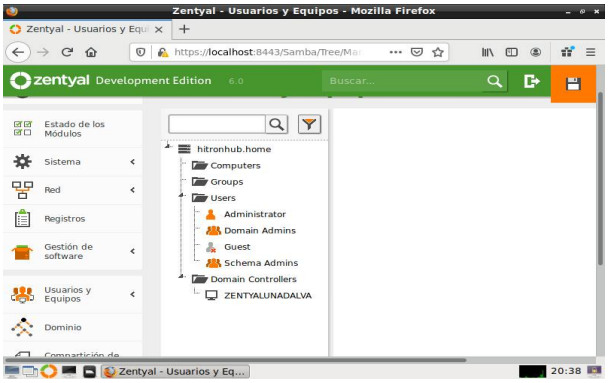

Imagen 40. Dominio, usuario y grupos configurados

Nos muestra el dominio, usuario y grupos a continuación, crearemos los usuarios.

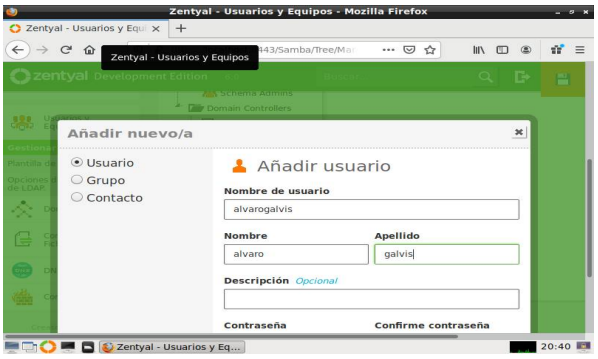

Imagen 41. Creación de usuario

Creo el usuario alvarogalvis con su respectiva contraseña.

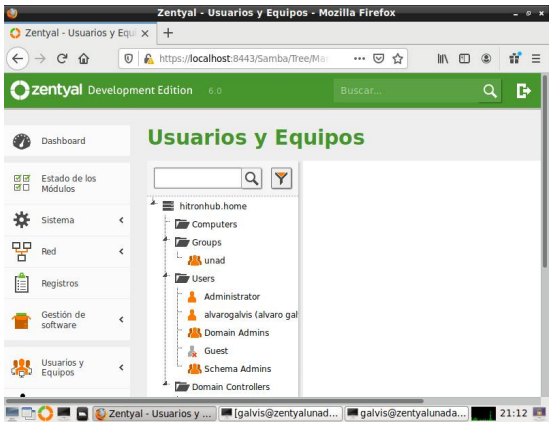

Imagen 42. Cuenta creada con éxito.

Queda creado el respectivo usuario.

Imagen 43. Solicitud de autenticación

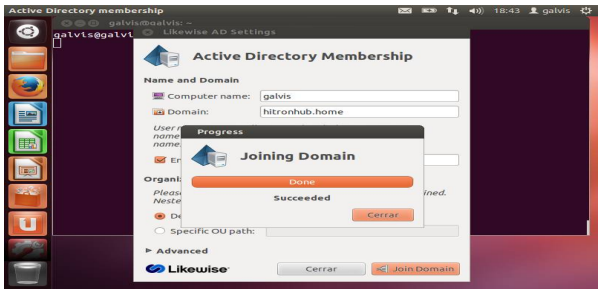

Imagen 44. Ingresando al Dominio.

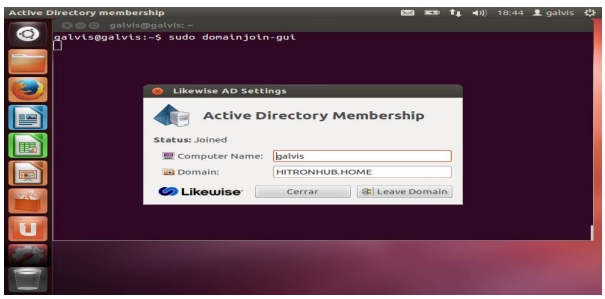

Imagen 45. Registro en el Active directory

Ejecutamos el comando sudo domainjoin-gui, el cual nos ejecutara likewise de manera gráfica para crear la conexión, agregamos nuestro dominio hitronhub.home, nuestro usuario creado anteriormente y su respectiva contraseña si el proceso es correcto nos muestra el mensaje done.

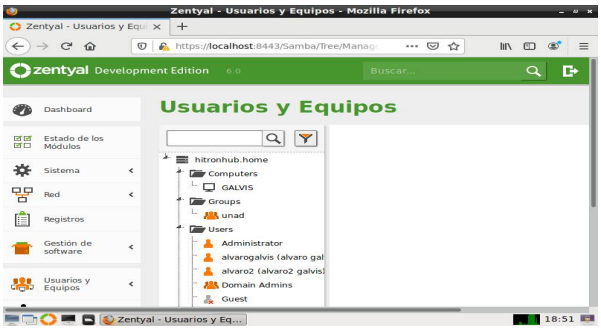

Imagen 46. Validación de conexión correcta

Se puede observar que el equipo con el nombre GALVIS aparece en computers lo que nos indica que la conexión fue exitosa.

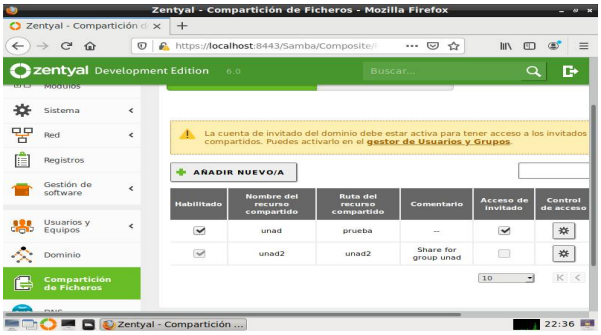

Imagen 47. Creación de archivos.

Creamos los archivos que vamos a compartir en compartición de ficheros, pero también desde usuario y equipos se puede crear ficheros y compartirlos con el usuario que creamos anteriormente.

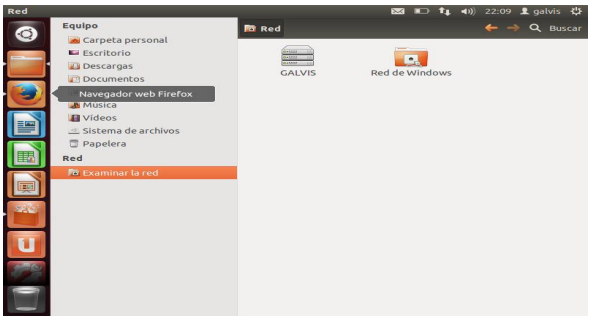

Imagen 48. Verificación del servidor

Vamos a red y vemos el servidor galvis.

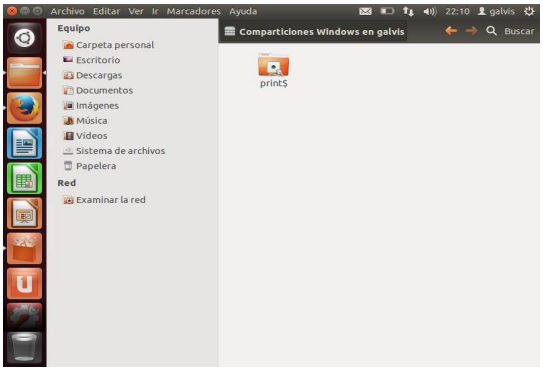

Imagen 49. Impresoras en red

Observamos la opción de impresoras en red.

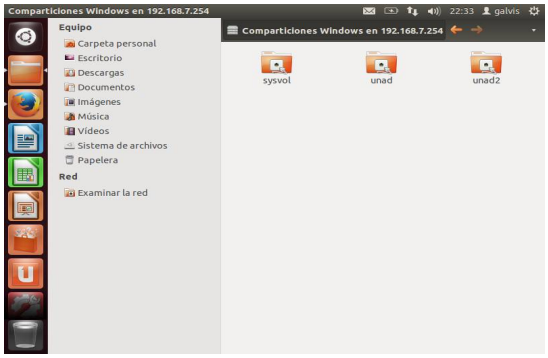

Imagen 50. Equipo cliente2.

Presionamos la tecla CTRL + la tecla l, nos aparece un buscador desde el equipo cliente2, se conecta con el servidor al recurso compartido con el comando smb://192.168.7.254. Nos muestra las carpetas creadas anteriormente en el servidor zentyal.

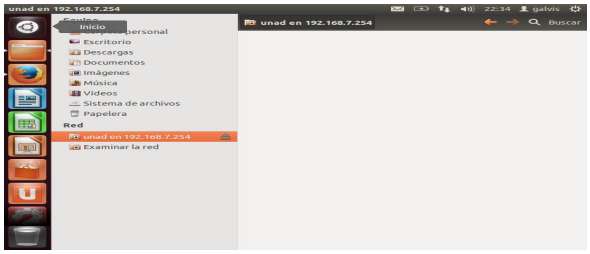

Imagen 51. Carpetas creadas.

Carpeta creada en Zentyal anteriormente visualizada desde Ubuntu.

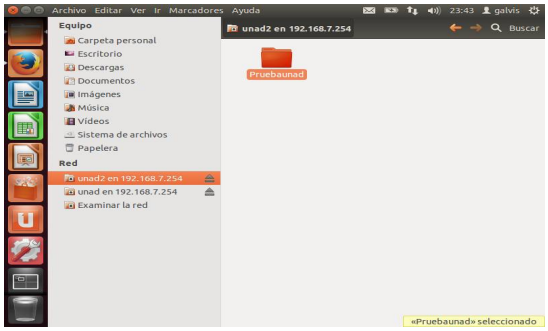

Imagen 52. Carpeta creada.

Creación de carpeta desde la estación Ubuntu, anteriormente se dio permisos desde Zentyal de escritura y lectura por eso el servidor me permite crear archivos en el servidor.

3.5 TEMÁTICA 5: VPN

Producto esperado: Implementación y configuración detallada de la creación de una VPN que permita establecer un túnel privado de comunicación con una estación de trabajo GNU/Linux Ubuntu Desktop. Se debe evidenciar el ingreso a algún contenido o aplicación de la estación de trabajo.

A continuación, debemos ingresar al menú de Autoridad de certificación/ crear certificado de autoridad, esto con el fin de crear con el fin de darle permisos a nuestro servidor para para crear certificados de seguridad, importante para la creación de certificados de acceso al servicio de VPN

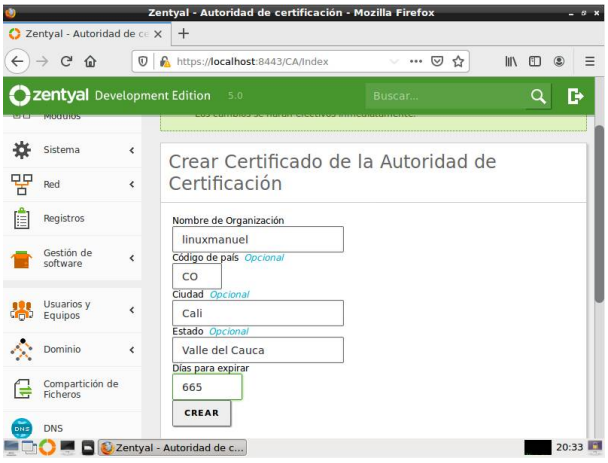

Imagen 53. Configuración de certificado de autoridad.

Debemos dirigirnos al menú principal y seleccionar la opción VPN/ servidores, en el añadiremos un servidor nuevo y se le coloca el nombre respectivo a este, se añade y a continuación, se guardan los cambios

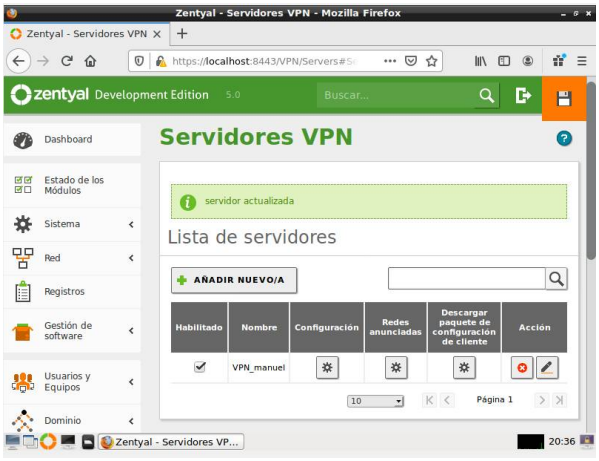

Imagen 54. Servidor creado

Nos dirigimos nuevamente al menú de certificados de autoridad/ general, y expedimos un nuevo certificado para el servidor VPN diligenciando su caducidad y el nombre que llevará, se presiona clic y el certificado se guardará automáticamente y se listará en la parte inferior con los demás certificados expedidos.

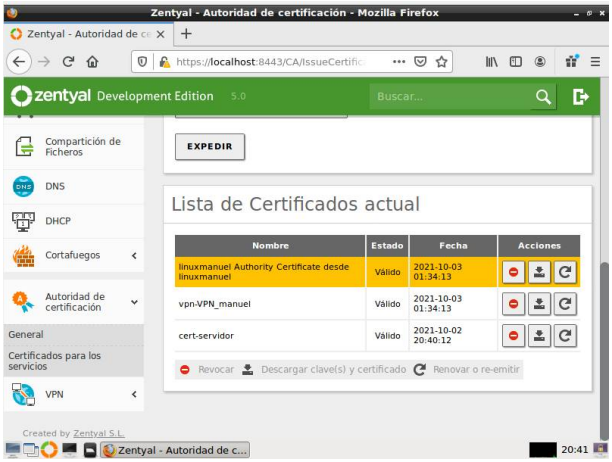

Imagen 55. Listado de certificados generados.

Regresamos nuevamente al menú de VPN/ Servidores, se observará el listado de servidores VPN creados, seleccionaremos el primero que se creó al comienzo en la opción de Configuración.

Una vez ingrese podrá observar los parámetros de configuración del servidor VPN como lo son el protocolo y puerto que se diligencias como UDP y 1194, la dirección VPN se deja por defecto, seleccionamos el certificado del servidor que creamos en el paso anterior, seleccionamos la opción TUN y por último en la opción de interfaz en la que escucha se deja en *"todas las interfaces de red"*, las demás opciones se dejan por defecto y a continuación damos en guardar...

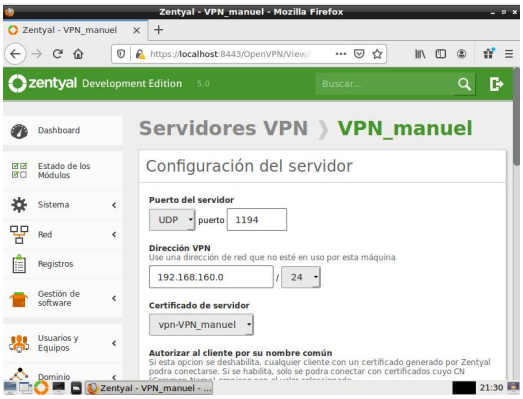

Imagen 56. Configuración de parámetros del servidor VPN.

Luego nos debemos dirigir al menú de Red/ Servicios para agregar un servicio de red, en este caso se agregará el de la VPN como tal, seleccionamos *"añadir nuevo"* e ingresamos el nombre del servicio a crear y la descripción, damos en el botón *"añadir"* y luego se guardan los cambios.

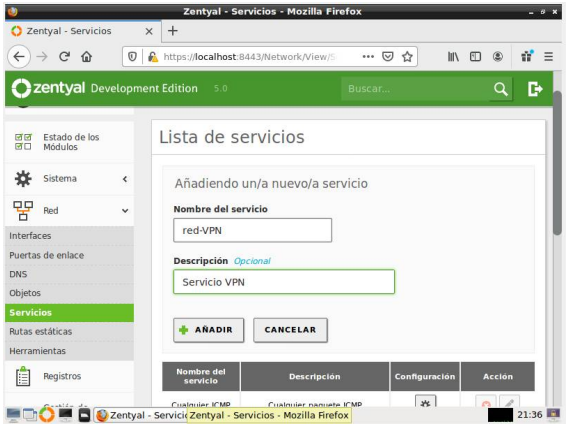

Imagen 57. Añadir un servicio de Red.

Una vez añadido se listarán los servicios creados y en dicha lista se encontrará el servicio recién añadido.

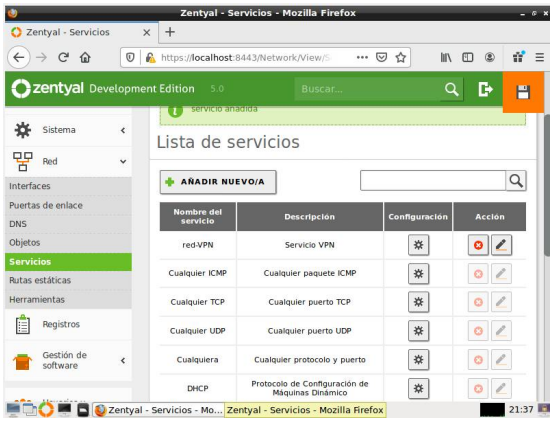

Imagen 58. Listado de servicios de Red.

Una vez ubicado el servicio creado, se presiona en el botón de configurar, donde se abrirá una opción para añadir la configuración del servicio, se da clic en *"añadir"*. A continuación, debemos parametrizar el protocolo de nuestro servicio en este caso UDP, el puerto de origen se selecciona *"cualquiera"* y en puerto destino seleccionamos *"puerto único"* y escribimos el número de puerto destino en este caso el 1194.y damos clic en *"añadir"* y luego en guardar para grabar los cambios generados.

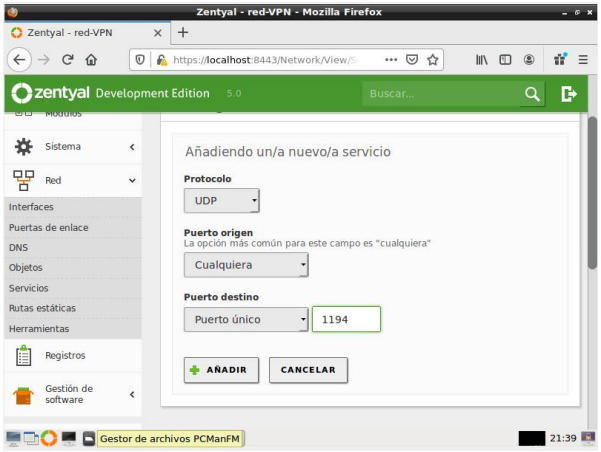

Imagen 59. Configuración del servicio de Red

Continuamos la configuración, ahora debe seleccionar del menú principal, la opción Firewall/ filtrado de paquetes, donde se procederá a crear una regla de excepción para el acceso al servidor, en dicho menú debemos seleccionar la opción de *"reglas de filtrado desde las redes internas a Zentyal"*, luego nos desplegara un listado de reglas ya parametrizadas en el firewall y daremos clic en *"añadir nuevo"*, luego nos pedirá que ingresemos la decisión de la regla, en este caso seleccionamos *"aceptar"*, el origen debe de ir la opción *"cualquiera"*.

Por ultimo seleccionamos el servicio de Red que creamos anteriormente de VPN y una descripción de la regla a ingresar, damos clic en añadir y guardamos los cambios.

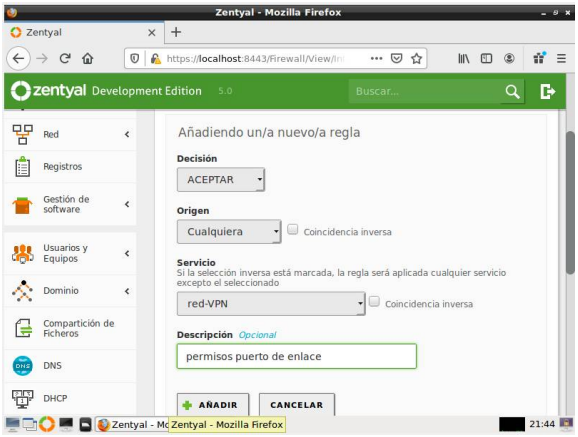

Imagen 60. Configuración de regla en el Firewall

Para finalizar el procedimiento, debemos regresar nuevamente al menú de VPN/ Servidores para validar si se encuentra parametrizada la *"red anunciada"* del servidor que creamos, en este caso el servidor creo una por defecto en la instalación, por lo que no es necesario crear una nueva.

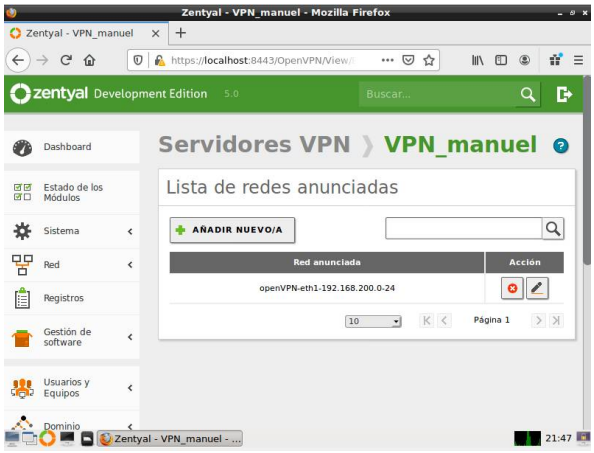

Imagen 61. Lista de redes anunciadas.

Una vez realizado los anteriores pasos, pasamos a crear el archivo de configuración de la VPN, el cual contiene la información referente a la Red que se va a conectar y a que servidor, protocolo y puerto va a acceder como tal, para ello debemos identificar inicialmente según la configuración del servidor, ¿Cuál es la dirección IP de acceso a internet (red WAN)? Y ¿cuál es la dirección local de nuestro servidor (red LAN)? Que esta parametrizada desde el enrutador principal.

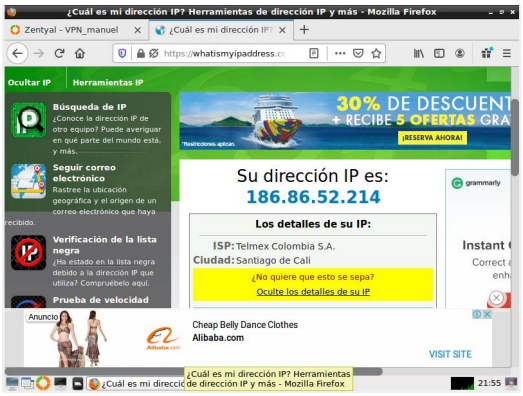

Imagen 62. Direccion IP de acceso a internet

Se tiene claro que las direcciones corresponden, WAN 186.86.52.214 y LAN 192.168.0.70, a continuación, se ingresa al menú de *"descargar paquete de configuración de cliente"* en el menú de VPN/ Servidores donde procederemos a ingresar la información de tipo de cliente (sistema operativo de la maquina que se conectará a la VPN) en este caso seleccionamos LINUX, certificado cliente se selecciona el certificado del servidor creado anteriormente, en dirección de servidor ira la dirección IP WAN consultada y la dirección LAN, para finalizar seleccionamos *"descargar"* y se bajara un archivo comprimido .GZ el cual compartiremos con el cliente que desea conectarse a la red por medio de una VPN.

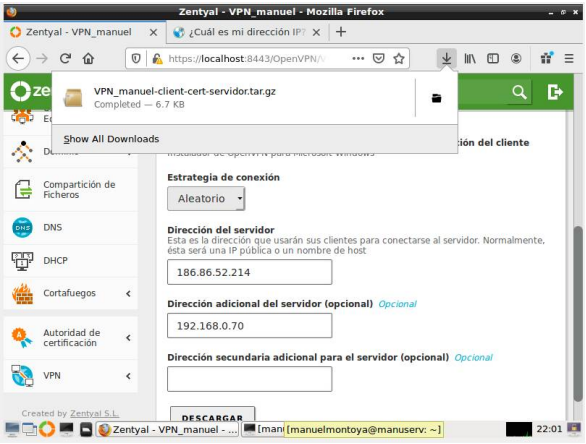

Imagen 63. Generar archivo de configuración de acceso a VPN

Finalizado el proceso, verificamos que el servicio este activo en el menú de dashboard en la parte inferior. Una vez conocido que el servicio está en línea vamos a la maquina cliente que se va a conectar a la VPN, y en caso de ser una distribución Ubuntu/ GNU/Linux deberemos activar en el menú de configuración el *"acceso universal"* para permitir la interacción de puertos con el servidor VPN. Abrimos la consola e instalamos openVPN con el comando *"sudo apt-get install openvpn",* ya finalizada la instalación procedemos a ingresar como usuario root en nuestra consola y nos situamos en la carpeta donde se encentra el archivo de configuración

de acceso de la VPN teniendo en cuenta que ya está descomprimido el archivo .gz, y la ejecutamos con el comando *"openvpn --config VPN_manuel-client.conf"* donde VPN_manuel-client.conf es el nombre del archivo de configuración y damos enter, podremos observar que efectivamente genera una conexión el servidor VPN que acabamos de configurar.

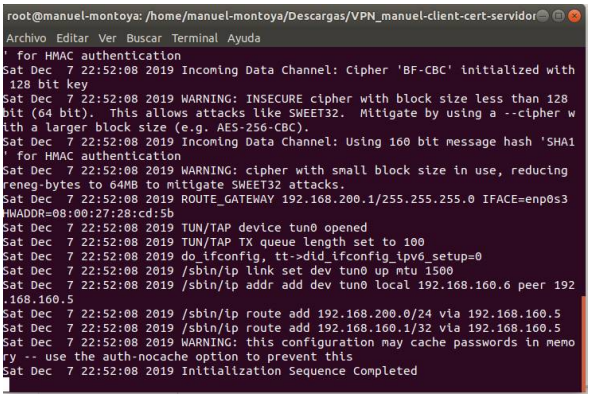

Imagen 64. Ejecución del archivo de configuración

Por ultimo validamos desde las entradas de Logs de control del servidor que nuestra maquina cliente allá accedido a la red, nos dirigimos desde el servidor Zential al menú de Registros/ VPN y en la parte inferior se encontrara el reporte que nos muestra el log de la conexión de la maquina cliente como se demuestra a continuación.

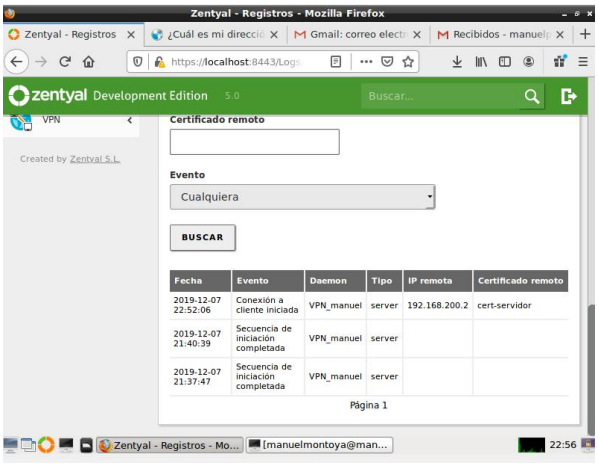

Imagen 65. Log de acceso a la VPN por parte del servidor

4 CONCLUSIONES

Se consiguió instalar y configurar el servidor Zentyal 5.0 como S.O, al igual que en con otros tipos de software como Endian, este permite un control muy amplio para gestionar una red.

Se aprendió a crear un server Proxy no transparente para administrar el tráfico de los equipos asociados a la red de trabajo por medio del puerto 3128.

Implementamos y configuramos detalladamente la creación de una VPN que permita establecer un túnel privado de comunicación con una estación de trabajo GNU/Linux Ubuntu Desktop. Evidenciamos el ingreso a algún contenido o aplicación de la estación de trabajo.

Se logró la creación de archivos en el servidor Zentyal y su respectiva visualización desde Ubuntu.

5 REFERENCIAS

[1] Osorio, R. [Rene Osorio]. (2018). *Proxy no transparente en Zentyal*. [Archivo de video]. [En línea]. Recuperado de: https://www.youtube.com/watch?v=4Yi0J7Xd7IQ

[2] [JGAITPro]. (2018). *Zentyal - Configuraciones iniciales de Red, DNS y Dominio*. [Archivo de video]. [En línea]. Recuperado de: https://www.youtube.com/watch?v=3pVd3a1utZo

[3] Caballero, M. [Manuel Cabrera Caballero]. (2018). *Zentyal Server | Instalación y primeros pasos*. [Archivo de video]. [En línea]. Recuperado de: https://www.youtube.com/watch?v=tG_NHAUYUbU

[4] *Primeros pasos con Zentyal*. (2018). [En línea]. Recuperado de: https://doc.zentyal.org/es/firststeps.html

[5] Zentyal Community. (2004). *Usuarios, Equipos y Compartición de ficheros*. [En línea]. Recuperado de: https://doc.zentyal.org/es/directory.html

[6] Ubuntu Documentation. (2011). *CUPS - Print Server*. [En línea]. Recuperado de: https://help.ubuntu.com/lts/serverguide/cups.html.en

[7] Zentyal Community. (2004) *Cortafuegos*. [En línea]. Recuperado de: https://doc.zentyal.org/es

[8] Lema, A. [Antonio de Andrés Lema]. (2015) *Configuración do firewall en Zentyal* [Archivo de video]. [En línea]. Recuperado de: https://www.youtube.com/channel/UCpEE3ayC4ZhKoa6Ww-yGpIA