PREPARACIÓN DEL REPORTE INFORME DE LABORATORIOS EN FORMATO DE DOS COLUMNAS (MANUSCRITO ESTILO “PAPER”).

William Camilo Mendieta Parra
wcmendietap@unadvirtual.edu.co
Jairo Andres Betancur Vélez
jabetancurv@unadvirtual.edu.co
Johan Andres Bolaños Puentes
jabolanospu@unadvirtual.edu.co
Jaime Alejandro Tirano Bernate
jatiranob@unadvirtual.edu.co

RESUMEN: *GNU / LINUX es un sistema de licencia libre, siendo una de sus características, permitir a los usuarios acceder a sus funcionalidades sin que eso implique una transacción comercial. Al ser de código abierto, 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. Este sistema operativo tiene herramientas de multiprocesamiento y multitarea, que permiten ofrecer ductilidad y versatilidad en funciones de seguridad, haciendo que se pueda aplicar a cualquier dispositivo informático. 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. 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 de identificaran los servicios utilizados, las ventajas y potencial que se puede tener, al saber administrar los diferentes servicios sobre las distribuciones de Linux.*

.

PALABRAS CLAVE: Terminal, Distribuciones Linux, Firewall, Proxy no transparente, proxy transparente, DNS, DHCP, Web services, Controlador de dominio, VPN, File server, user root, antivirus, puertos, local host, seguridad informática.

1 INTRODUCCIÓN

La presente actividad tiene como fin complementar los conocimientos fundamentales para el desarrollo del curso de Diplomado De Profundización En Linux (Opción De Trabajo De Grado), familiarizando de una manera práctica y didáctica a los alumnos, garantizando así la adquisición de destrezas, enfocado directamente en interpretar, identificar, aplicar y aprender en forma clara el Afinamiento de contenidos sobre GNU/Linux y el alistamiento del server para aplicar lo aprendido en el curso. Todo esto se lleva a cabo con el material indicado por la universidad, logrando así que tome una importancia para el estudiante conocer estos procedimientos, conceptos y terminología empleada. En este informe se muestran imágenes con el objetivo de poder ilustrar los procedimientos realizados por cada uno de los integrantes del equipo de trabajo, donde se evidencia el desarrollo de cada una de las temáticas de una forma clara, además de la apropiación de los conceptos aprendidos a lo largo del diplomado.

Con base en lo anterior se utilizará Zentyal server para la administración de la infraestructura de red y sus servicios asociados, tales como: DHCP, DNS, Controlador de dominio, Proxy transparente, Firewall, File Server, Print Server y VPN. Estos serán los servicios que se instalarán y configurar en este informe.

2 INSTALACION DE ZENTYAL

Zentyal es un servidor que permite administrar a través de un navegador web diferentes servicios (Gestión de Red, comunicaciones, compartición de recursos, gestión centralizada de usuarios, etc.) este sistema está basado en Ubuntu.

Lo primero que se debe realizar es descargar la imagen .iso desde url: https://zentyal.com/es/trial-gratuito-de-45-dias-del-servidor-zentyal/ donde aparece un formulario que se debe llenar, una vez realizamos este procedimiento recibiremos un correo electrónico con el serial trial y la url de descarga del archivo .iso.

Para realizar la instalación realizamos lo siguiente:

1. Creamos la máquina virtual en Virtual Box.

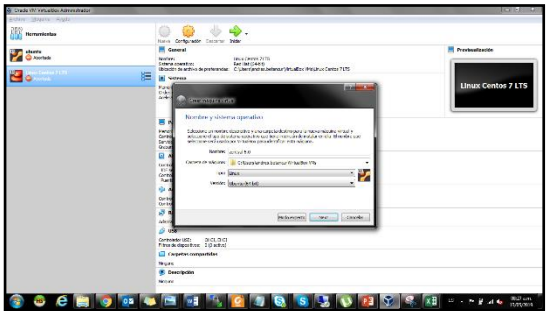


Fig 1. Creación de máquina virtual.

2. Asignamos capacidad de memoria RAM y disco duro a la máquina Virtual.

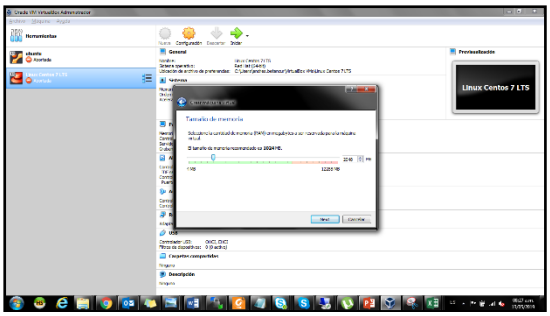


Fig 2. Asignación de memoria RAM a máquina virtual.

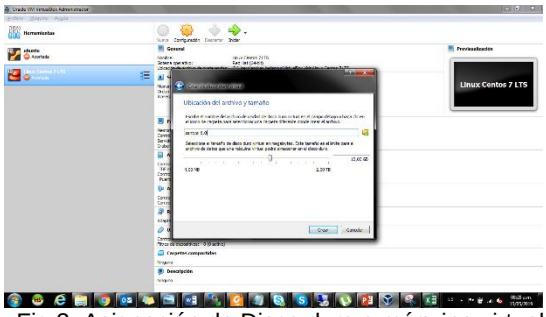


Fig 3. Asignación de Disco duro a máquina virtual.

3. Elegimos la imagen .ISO para la instalación.

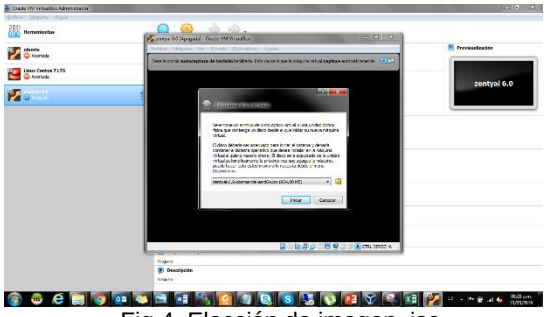


Fig 4. Elección de imagen .iso.

4. Elegimos el tipo de instalación de Zentyal.

Fig 5. Tipo de instalación.

5. Seleccionamos el idioma de instalación y continuamos con el proceso de instalación.

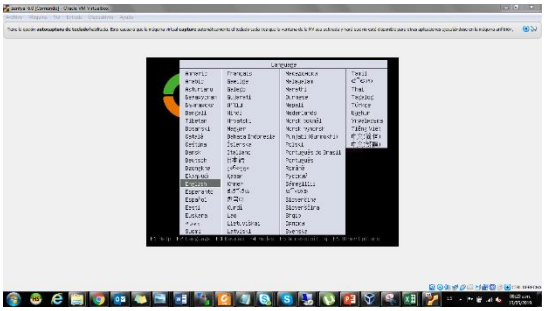


Fig 6. Elección de idioma.

6. Seleccionamos el país.

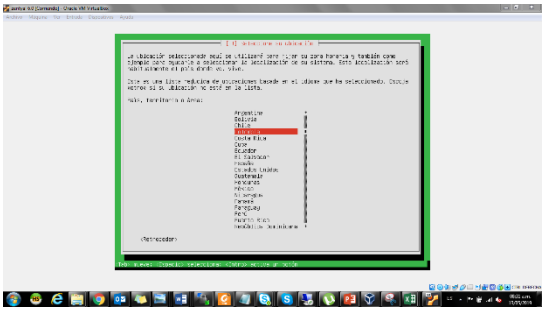


Fig 7. Elección del país.

7. Luego seleccionamos el idioma del teclado.

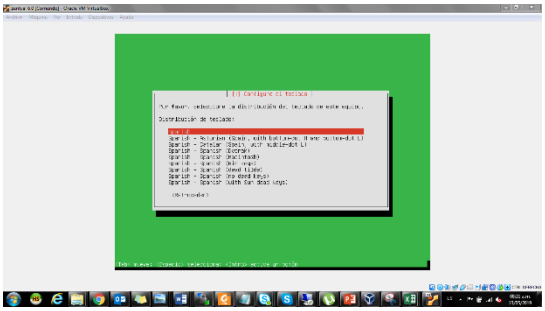


Fig 8. Elección del idioma para el teclado.

8. Ahora procedemos a colocarle un nombre a la maquina.

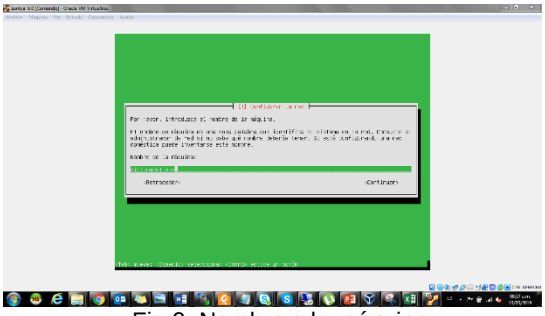


Fig 9. Nombre a la máquina.

9. Se debe colocar el nombre de usuario y contraseña para posterior logeo.

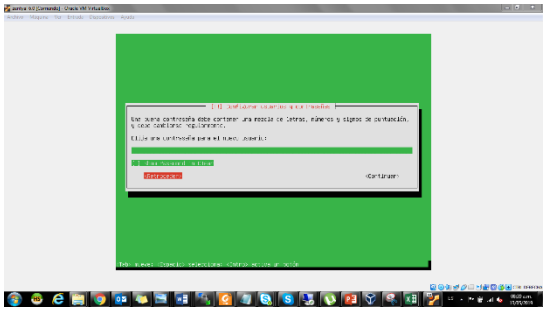


Fig 10. Nombre de usuario y contraseña.

10. Después de dar en continuar, la instalación empieza, al finalizar muestra un mensaje que ha terminado la instalación.

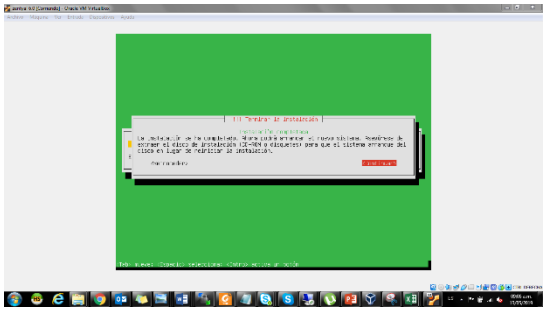


Fig 11. Mensaje de finalización de la instalación.

Una vez realizada la instalación del servidor Zentyal, este abrirá una página web en el navegador permitiendo realizar la instalación de los diferentes servicios y posterior administración de los mismos.

3 TEMATICAS

Las temáticas a desarrollar se tomaron de acuerdo a la guía de actividades dispuesta en este paso 8 del Diplomado, a continuación, se describen:

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.

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.

Temática 3: 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 del Funcionamiento del cortafuego aplicando las restricciones solicitadas, se hará desde una estación de trabajo GNU/Linux Ubuntu Desktop.

Temática 4: File Server y Print Server.
Producto esperado: Implementación y configuración detallada del acceso de una estación de trabajo GNU/Linux Ubuntu Desktop a través del controlador de dominio LDAP a los servicios de carpetas compartidas e impresoras.

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.

4 Resultados

4.1 TEMÁTICA 1 – DHCP server – DNS server y controlador de dominio

1. Iniciamos sesión con las credenciales antes puestas.

Figura 12. Inicio de sesión.

2. Colocamos la licencia antes enviada al correo.

Figura 13. Clave de activación Trial

3. Después de esto, se abre la configuración inicial.

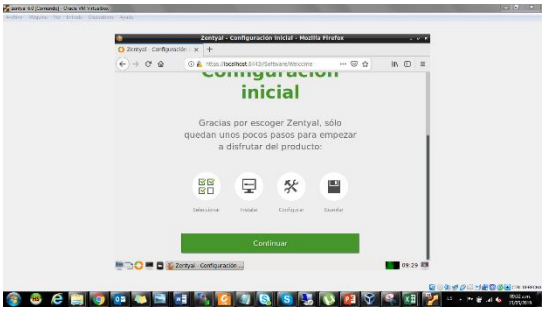


Figura 14. Pantalla de configuración inicial.

4. Se seleccionan los módulos que queremos instalar.

Figura 15. Módulos Zentyal.

5. Inicia la instalación de los módulos.

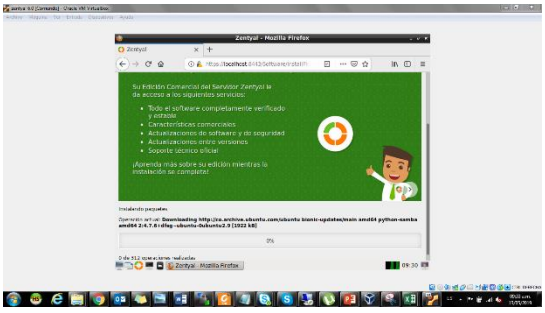


Figura 17. Instalación módulos.

6. Elegimos la opción de ip static.

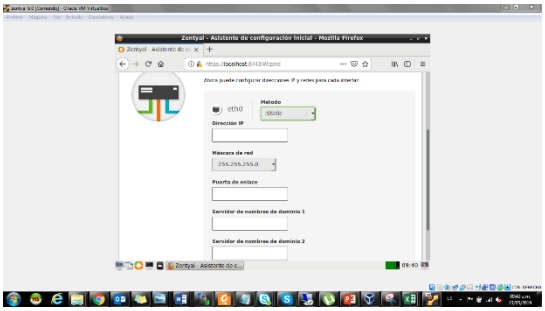


Figura 18. Configuración de IP.

7. Colocamos el nombre al dominio.

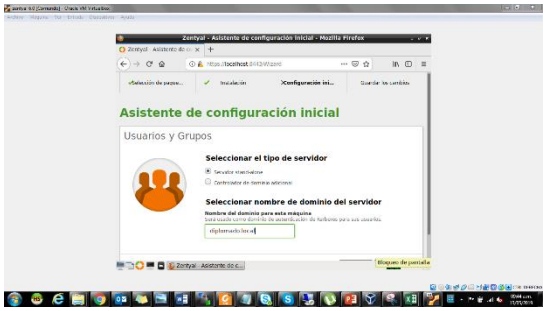


Figura 20. Configuración de dominio.

8. Procedemos a habilitar los servicios

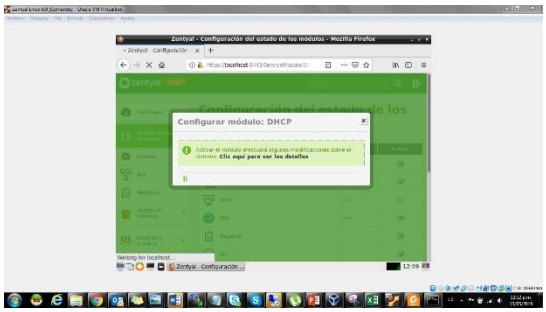


Figura 21. Habilitación de módulos.

9. Damos clic en guardar.

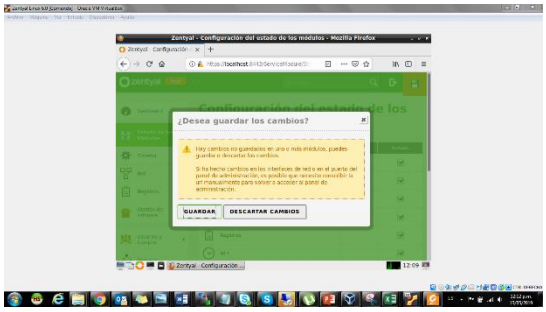


Figura 22. Guardar configuración.

10. Es necesario realizar algunos cambios en la configuración de las tarjetas de red en Virtual-Box.

- El primer cambio es dejar el adaptador 1 como NAT.

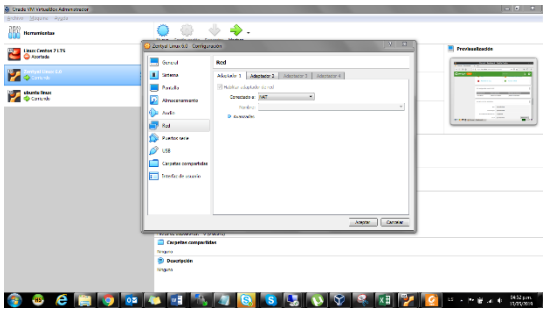


Figura 23. Configuración tarjeta de red.

- El segundo cambio es dejar el adaptador 2 como red interna.

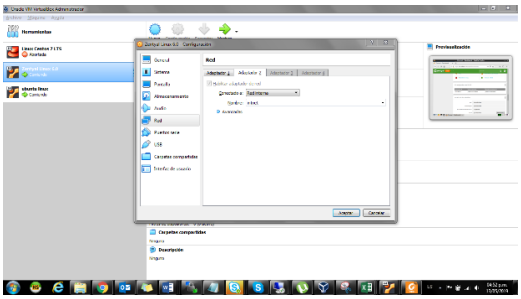


Figura 24. Configuración tarjeta de red.

- Lo mismo hacemos en la maquina con Ubuntu.

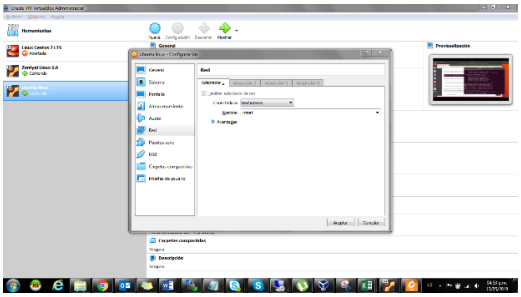


Figura 25. Configuración tarjeta de red Ubuntu

11. Después de configurar los adaptadores se procede a configurar el servicio DHCP en el servidor.

- Para ello se debe dejar el eth0 por DHCP.

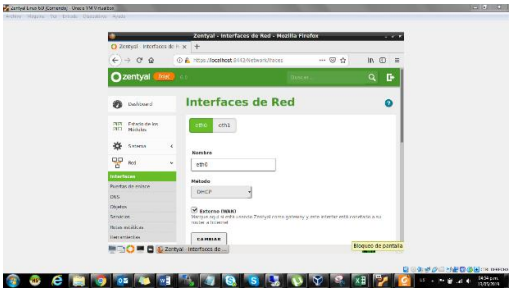


Figura 26. Configuración eth0.

- El eth1 se le va a asignar una IP fija.

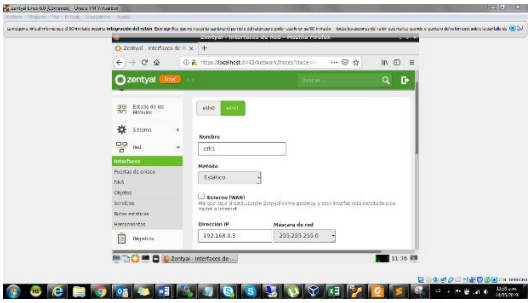


Figura 27. Configuración eth1.

12. Ahora en el módulo DCHP asignamos los rangos.

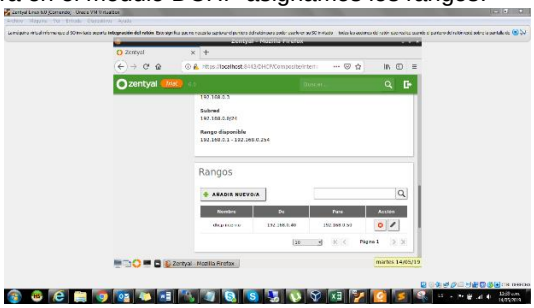


Figura 28. Asignación de rangos DHCP.

13. Realizando estos cambios, se observa el equipo asignado por DCHP.

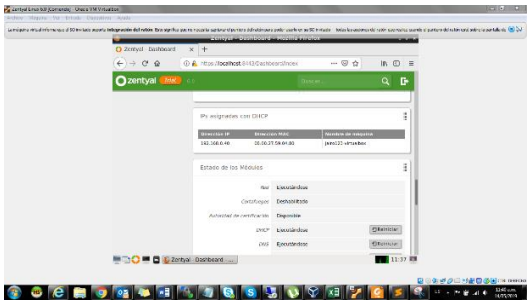


Figura 29. Evidencia equipo Ubuntu DHCP.

14. Una vez realizada la configuración del DCHP y de realizar todas las validaciones procedemos a validar que nuestro dominio este correctamente configurado.

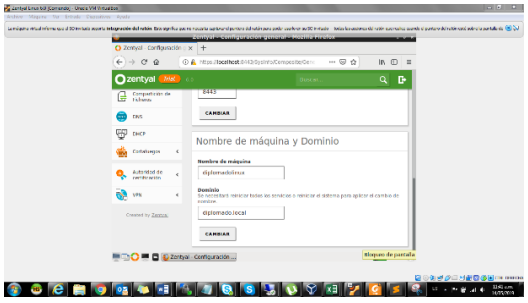


Figura 30. Validación dominio.

15. Validamos desde la maquina con Ubuntu que responda nuestro servidor con Zentyal.

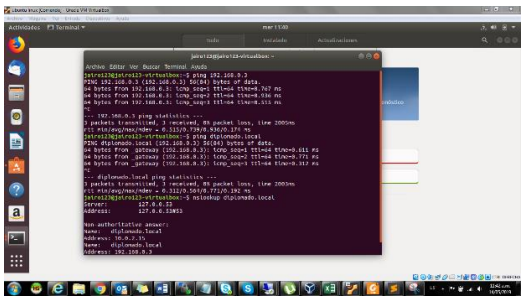


Figura 31. Ping al servidor Zentyal desde Ubuntu desktop.

16. Validamos las configuraciones de nuestro DNS.

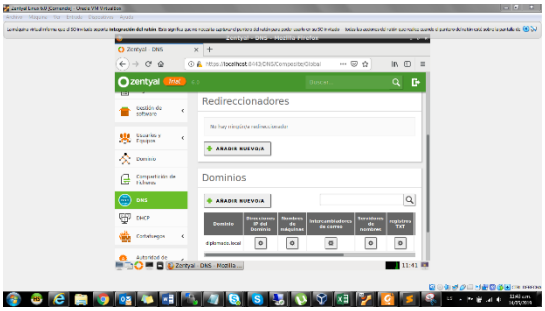


Figura 32. Validación DNS.

17. Después de esto se procede con la creación del usuario AD.

- Se abre la pestaña Usuarios y equipos – añadir usuario.

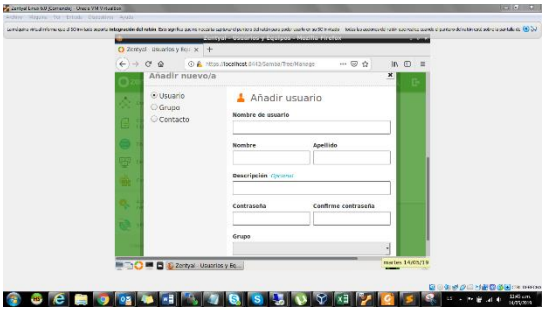


Figura 33. Creación usuario AD.

- Se debe llenar los datos que aparecen allí y dar clic en Añadir, después de esto el usuario quedara creado, importante: se debe añadir al grupo de administradores.

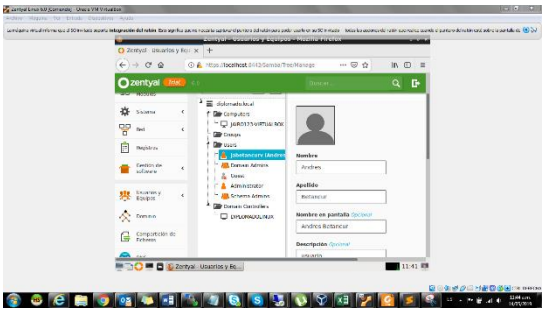


Figura 34. Validación de usuario creado.

Nota: *Se deben guardar todos los cambios realizados.*

18. Una vez creado el usuario en el Directorio Activo, se procede a unir la maquina con Ubuntu al dominio. Para esto se necesita instalar PBIS el cual nos permitir agregar la maquina al Zentyal.

- Se realiza la descarga del agente.

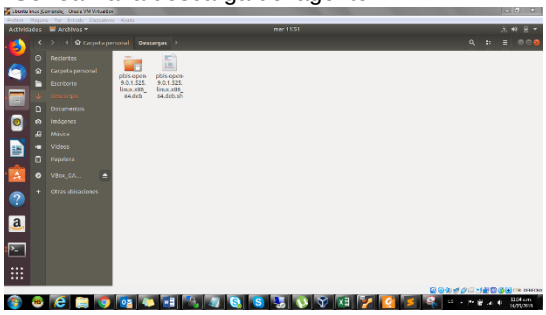


Figura 35. PBIS descargado.

- Se procede a instalar, para ello se debe dar permisos con el comando: $ sudo chmod a+x pbis-open-8.2.... después si ejecutamos el comando $ sudo ./pbis-open-8.2.1.2979.linux.x86_64.deb.sh.

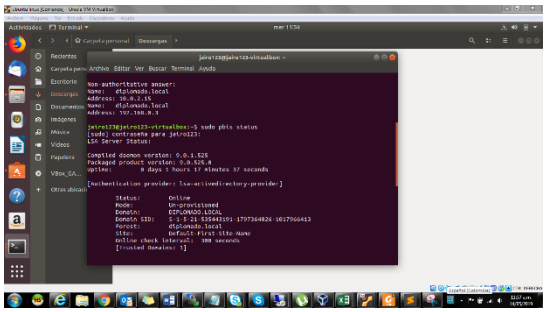


Figura 36. Instalación de PBIS en Ubuntu.

19. Después de instalado el programa, procedemos a unir el Ubuntu al dominio con el comando sudo /opt/pbis/bin/domainjoin-cli join diplomado.local Administrator@movich.local.

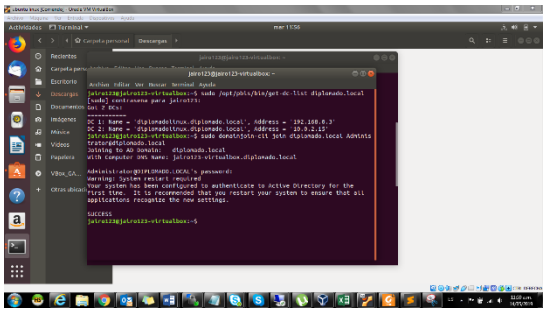


Figura 37. Evidencia equipo añadido al dominio.

Se puede evidenciar que esta añadido al dominio, ahora debemos reiniciar la máquina para que se apliquen los cambios.

20. Para finalizar validamos el inicio de sesión en la maquina con Ubuntu.

- Ingresamos con el usuario creado que es: jairo123betancur@diplomado.local y contraseña: 123456.

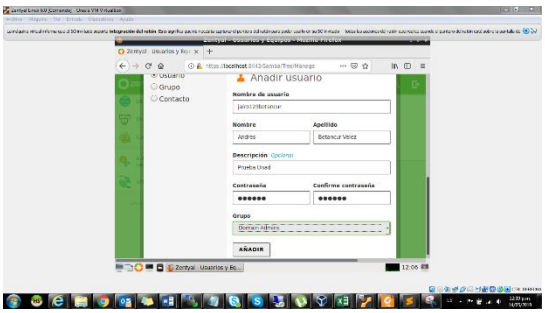


Figura 38. Validación de usuario creado.

- Ingresamos los datos de inicio Usuario: jairo123betancur@diplomado.local.

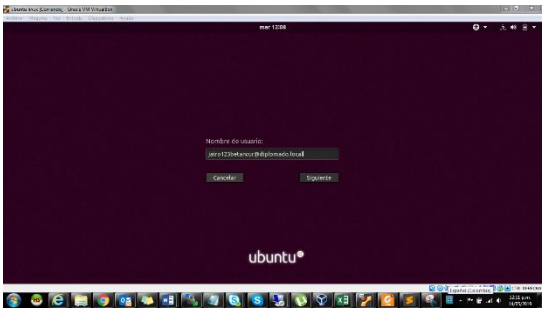


Figura 39. Ingreso de usuario de dominio en Ubuntu.

- Validamos el acceso exitoso.

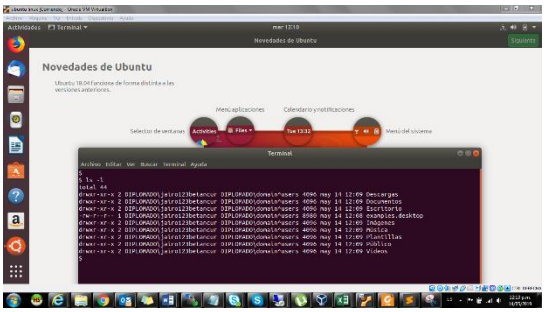


Figura 40. Validación de acceso exitoso.

4.2 TEMÁTICA 2 –Proxy no transparente

En el entorno web podemos hacer la instalación de paquetes disponibles, este se realiza el login con el usuario y la contraseña configurada en la instalación.

1. Portal de gestión Zentyal.

Figura 41. Acceso web.

2. A través de este entorno web podemos hacer la instalación del Proxy HTTP.

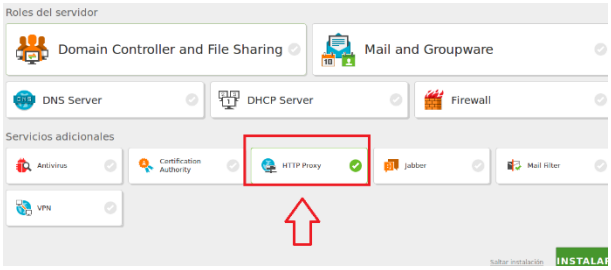


Figura 42. Modulo proxy.

3. Luego de la instalación vamos al dashboard para hacer la configuración del proxy http y seleccionamos la opción “General Settings”.

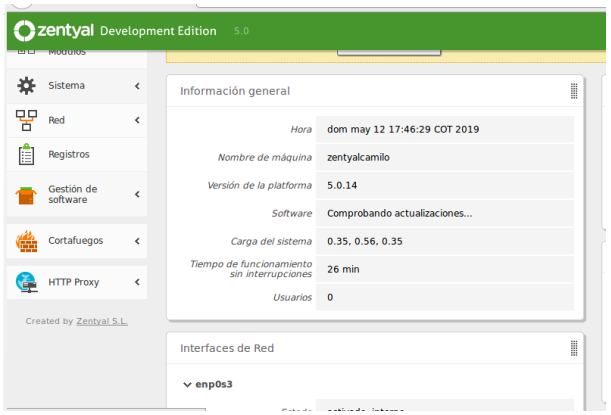


Figura 43. Configuración proxy.

4. El sistema nos indica que el modulo http proxy esta desactivado y nos la opción de hacer la activación.

Figura 44. Activacion modulo proxy.

5. Una vez el proxy habilitado continuamos con la configuración de las reglas para el acceso a contenidos en internet.

   - En el campo “periodo de tiempo” se especifica en qué momento se aplicará la regla.
   - En el campo “origen” seleccionamos si se aplicara a los miembros de un Objeto de Zentyal o a cualquier tipo de tráfico que atraviese el proxy.
   - En el campo “decisión”, existen 3 opciones de selección, permitir todo, denegar todo y aplicar filtros, seleccionamos la última.

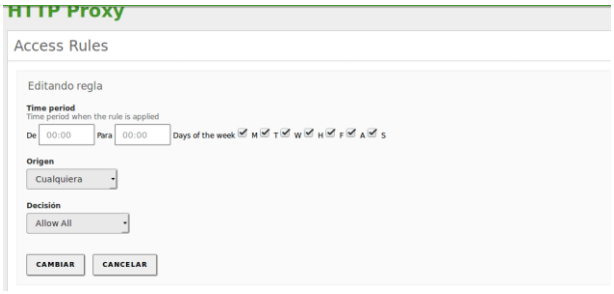


Figura 45. Configuración parámetros proxy.

6. Seleccionamos el perfil de “Filter profiles ” le damos un nombre al filtro que vamos configurar.

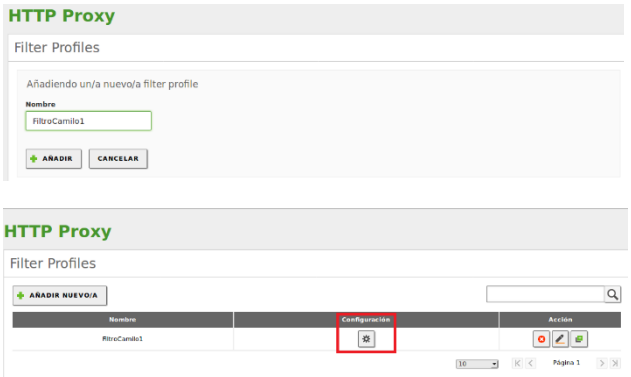


Figura 46. Nombre de filtro.

7. La primera pestaña nos muestra el umbral de contenido.

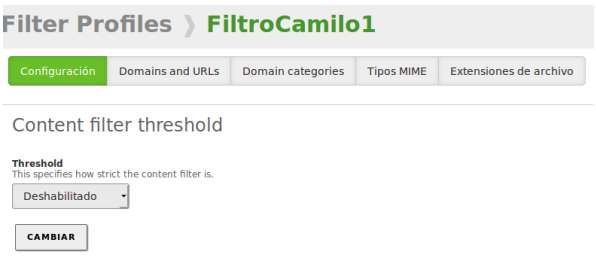


Figura 47. Configuracion de filtros.

8. Seleccionamos una opción de configuración, así mismo el sistema nos avisara que el módulo de antivirus debe ser activado para poder usarlo.

Figura 48. Módulo de dominios.

9. Configuración de las páginas a establecer, junto con la decisión de permitir o denegar el acceso.

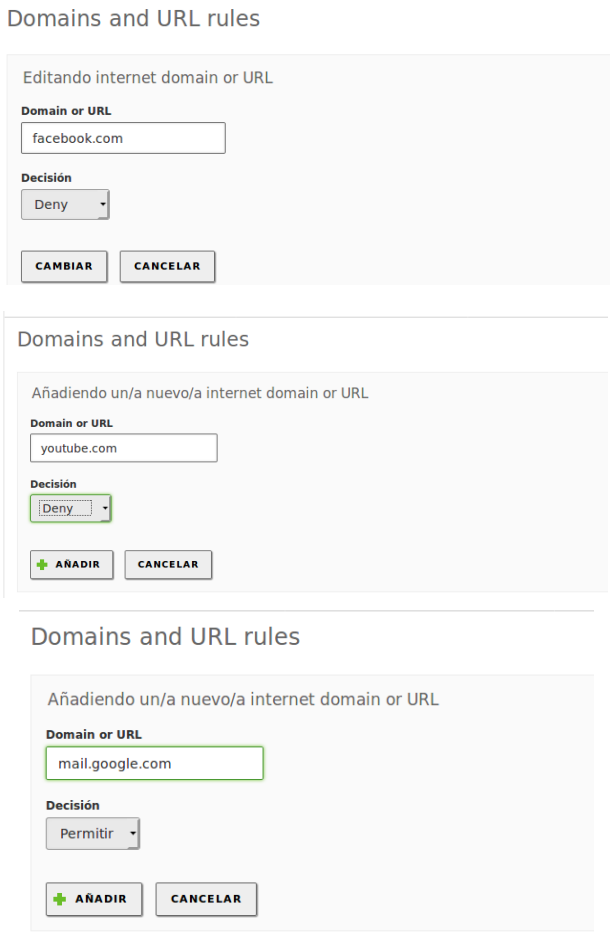


Figura 49. Configuracion de dominios.

10. Verificar configuracion realizada.

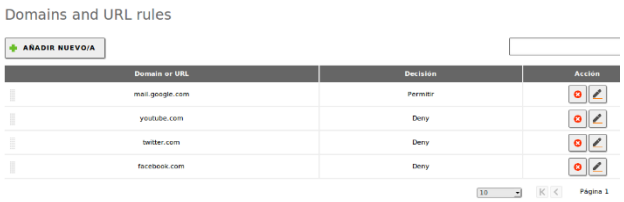


Figura 50. Dominios .

11. Aplicar el filtro a las reglas de acceso.

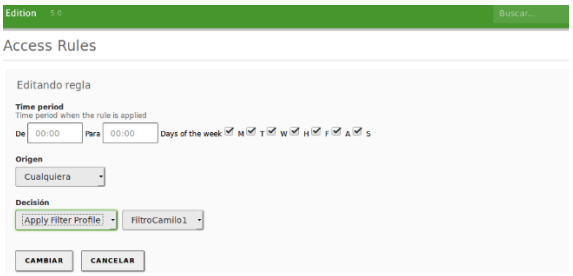


Figura 51. Aplicación de regla.

12. Pruebas sobre navegador en desktop.
Configuración sobre el navegador Mozilla del desktop el proxy configurado con la dirección ip y el puerto 3128.

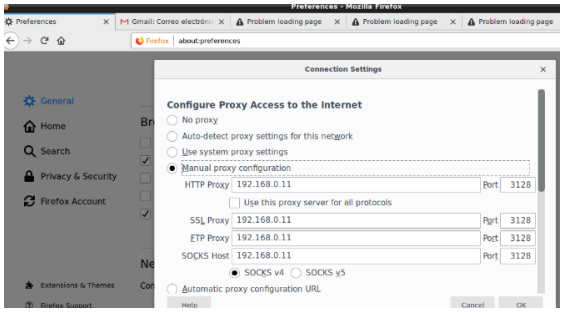
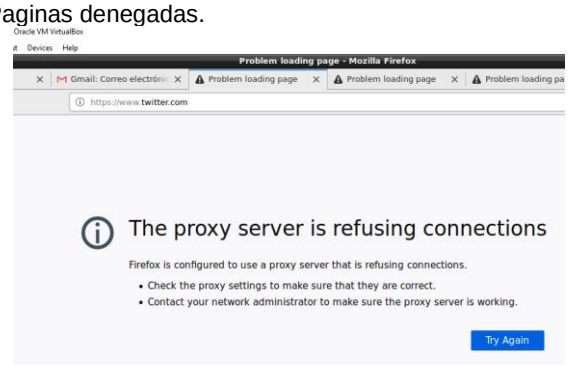
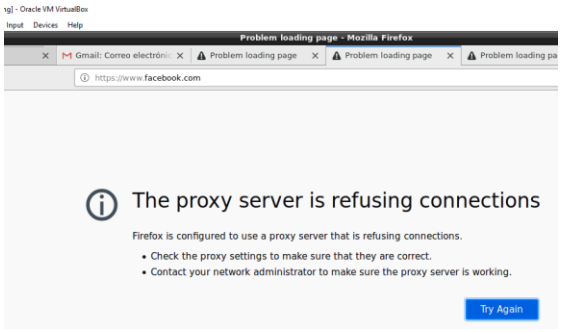


Figura 52. Proxy desktop

13. Pruebas sobre las páginas web configuradas
Paginas denegadas.





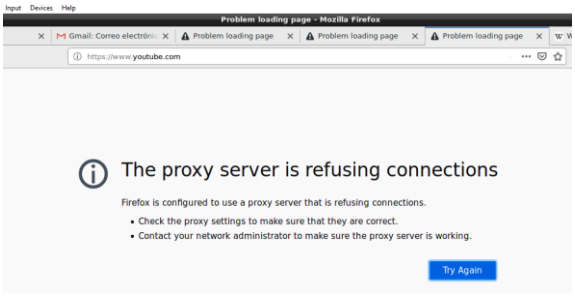


Figura 53. Paginal bloquedas.

Paginas permitidas.

Figura 54. Pagina permitida.

4.3 TEMÁTICA 3 - Cortafuegos

Figura 55.

1. Se carga la configuración inicial del servidor Zentyal, esta se produce inmediatamente se inicia el servidor.

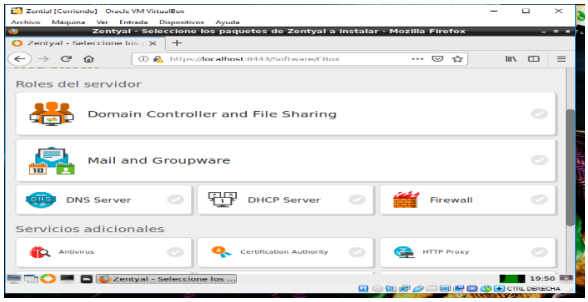


Figura 56

2. Se verifica el correcto funcionamiento del Panel de Configuración del servidor Zentyal.

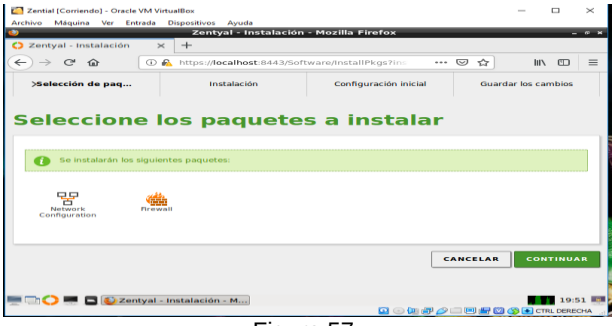


Figura 57.

3. Se procede a seleccionar los paquetes requeridos de acuerdo al tipo de actividad, para su posterior proceso de instalación.

Figura 58.

4. Se inicia el proceso de Instalación de paquetes requeridos para cumplir con la actividad.

Figura 59.

5. Se procede a acceder a la selección interfaz red, con la finalidad de seleccionar la interfaz de conectividad con la que se cuenta.

Figura 60.

6. Se configura la opción de detecciones IP, mediante el método de asignación DHCP.

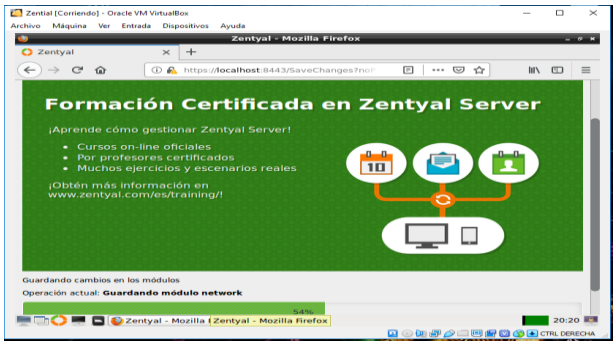


Figura 61.

7. Se procede con la configuración de las características seleccionadas con anterioridad.

Figura 62.

8. Se comprueba la finalización de la instalación y configuración de componentes que habían sido seleccionados.

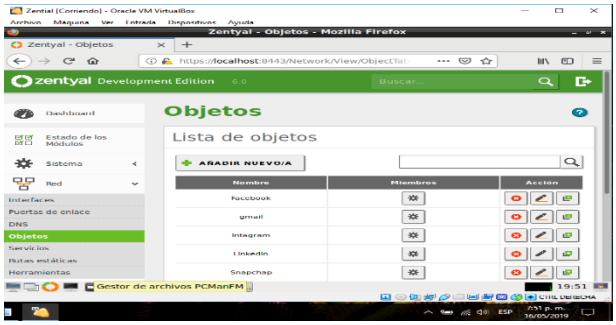


Figura 63.

9. En la opción del módulo red - objetos, se procede a agregar los objetos con las IP de los sitios que han sido seleccionados a restringir su acceso.

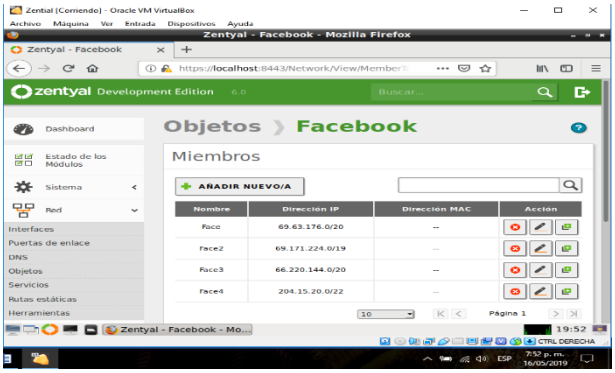


Figura 64.

10.Se debe configurar a cada objeto los miembros con los que cuenta y en los cuales se especifican la IP y la máscara de subred.

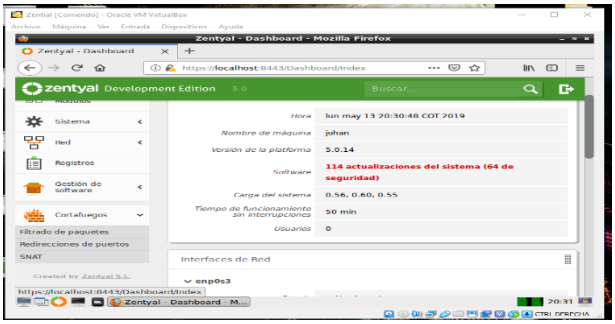


Figura 65.

11. se procede a seleccionar la opción de Cortafuegos y filtrado de paquetes, para las posteriores configuraciones.

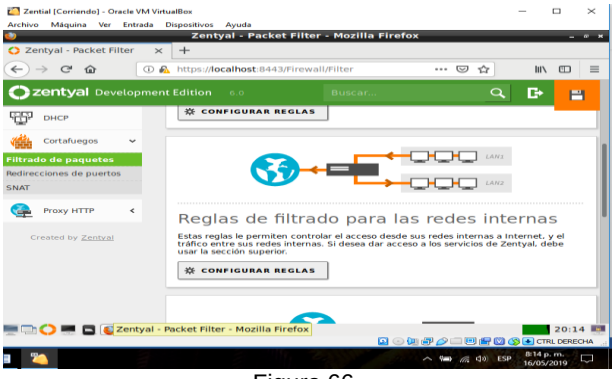


Figura 66.

12. Se procede a seleccionar la opción de reglas de filtrado para las redes internas.

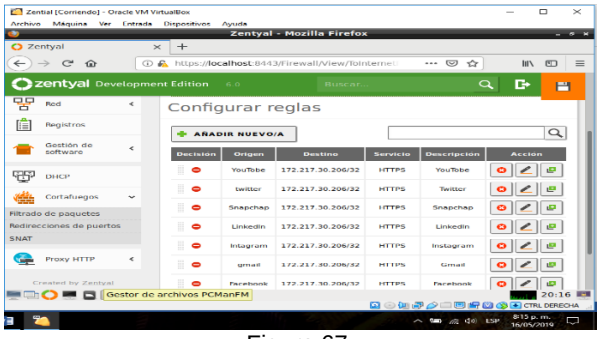
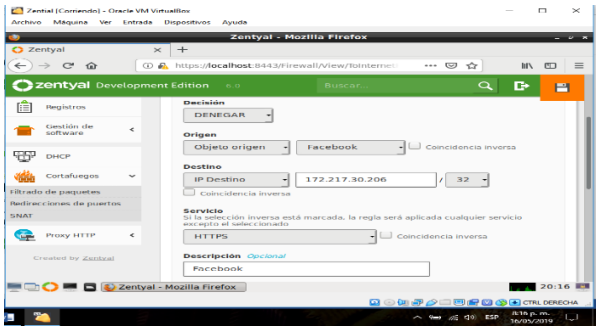


Figura 67.

13. Se procede a crear las reglas de filtrado, estipulando el tipo de servicio, el origen y el destino de la restricción de los sitios web.



Figuro 68.

14. Regla de filtrado Facebook.
En las reglas creadas se estipula que se deniega el servicio por HTTPS a las ips de los sitios seleccionados, posterior a esto re direcciona a la ip de Google.com (172.217.30.206).

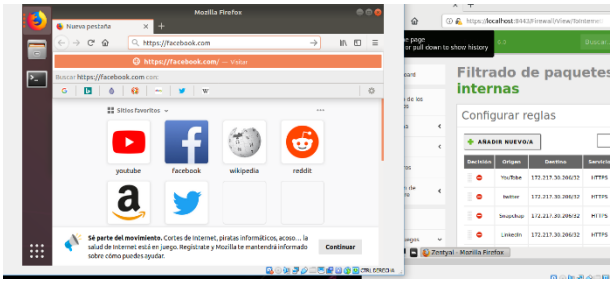


Figura 69.

15. Se procede a verificar desde máquina virtual con sistema operativo Ubuntu, la cual cuenta con el mismo segmento de asignación IP.

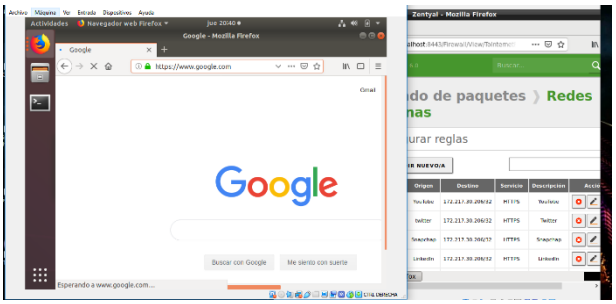


Figura 70.

16. Se verifica desde maquina con sistema operativo Ubuntu, evidenciando el redireccionamiento a la IP de Google.

4.4 TEMÁTICA 4 - File Server y Print Server

1. Para realizar esta configuración es necesario tener nuestro sistema Ubuntu desktop añadido al dominio.

Nota: esta actividad ya se desarrolló en la temática 1.

2. Ingresamos a la opción de compartición de ficheros y damos clic en Añadir Nuevo.

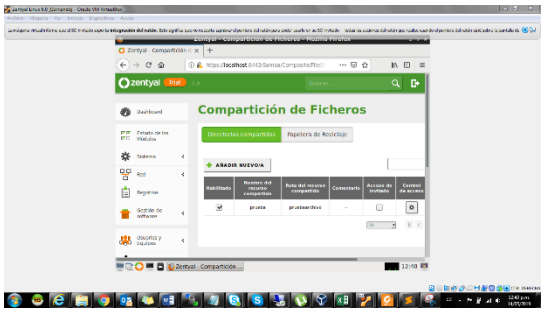


Figura 71. Nuevo fichero

3. Ingresamos los datos para crear el archivo que queremos compartir y damos clic en añadir.

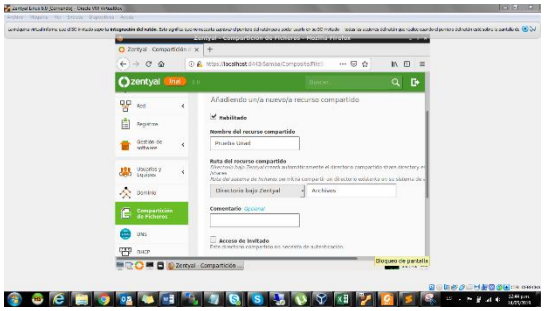


Figura 72. Nuevo archivo creado.

4. Una vez creado, damos clic sobre control de acceso.

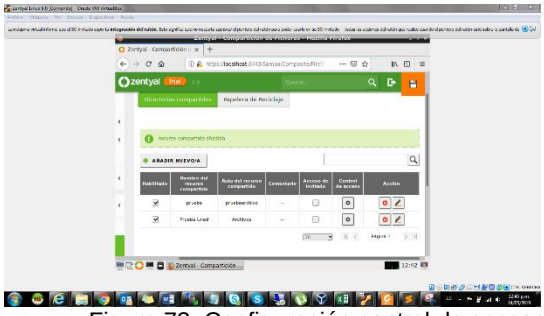


Figura 73. Configuración control de acceso.

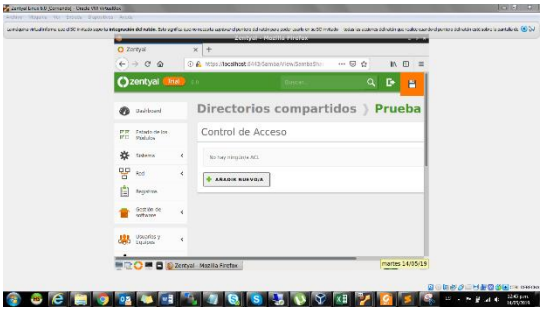


Figura 74. Control de acceso creado.

5. Damos clic sobre añadir nuevo y después seleccionamos el usuario y los permisos que deseamos dar.

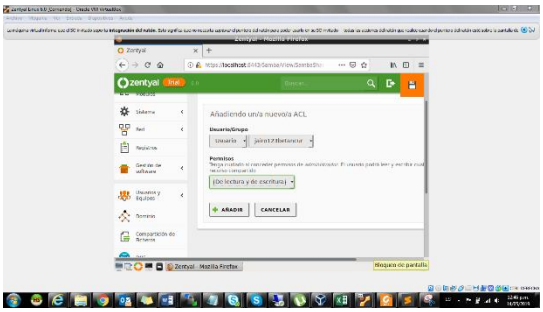


Figura 75. Asignación de permisos.

6. Damos clic en guardar.

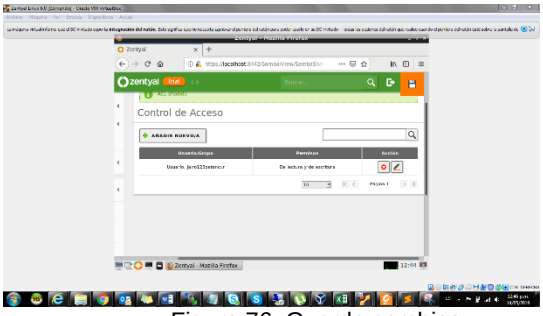


Figura 76. Guarda cambios.

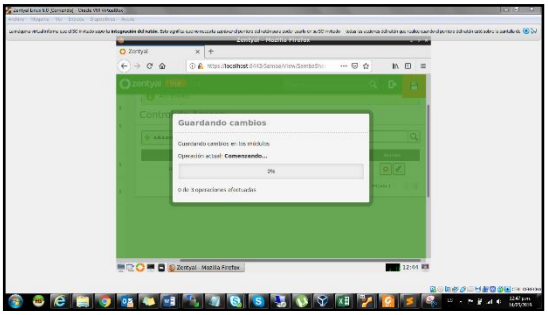


Figura 77. Configuración guardada.

7. Validamos el acceso a la carpeta creado desde el equipo Ubuntu.

Ingresamos los datos smb://192.168.0.3/ y damos clic en conectar.

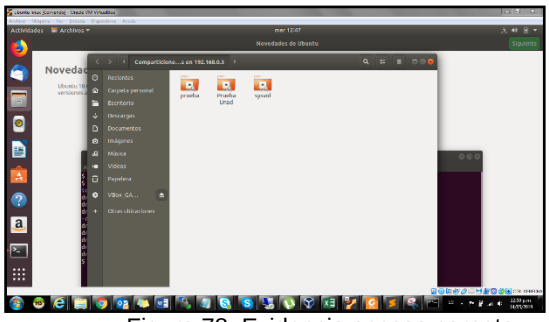


Figura 78. Evidencia acceso carpeta compartida.

Aparecen las carpetas creadas, al dar clic sobre ellas nos pide autenticación, donde ponemos los datos de inicio de sesión y todo estaría bien.

4.5 TEMÁTICA 5 – VPN

1. Una vez se ha instalado el sistema operativo seguimos con la configuración para instalar el paquete que nos va a permitir hacer la configuración e implementación de una VPN.

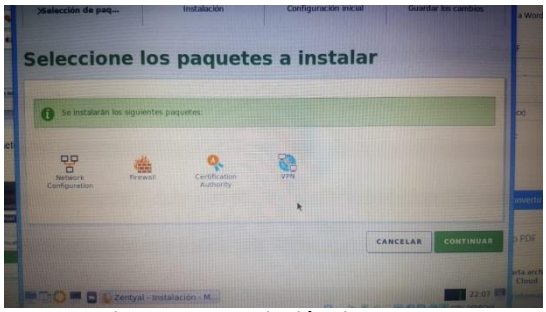


Figura 79. Instalación de paquete VPN.

2. Ahora comenzamos con la configuración del servidor VPN y los certificados que vamos a utilizar para realizar el túnel privado de comunicación. Vamos al menú autoridad de certificación

   En el menu desplegable seleccionamos general aparecera, la informacion EXPEDIR UN NUEVO CERTIFICADO le indicamos el nombre del certificado que puede ser el que se quiera. y luego EXPEDIR .

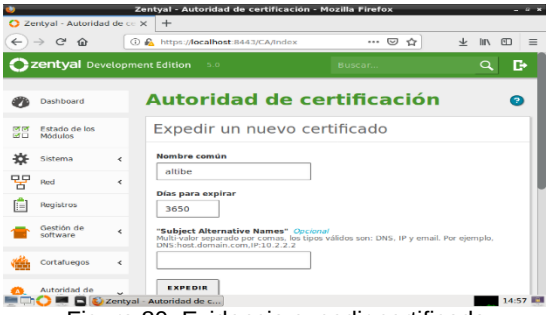


Figura 80. Evidencia expedir certificado

3. Después vamos a la sección VPN y Clientes - lista de servidores AÑADIR NUEVO se da un nombre y AÑADIR.

Figura 81. Añadir servidor.

4. Verificamos el estado del srvidor en la pestaña Dashboard.

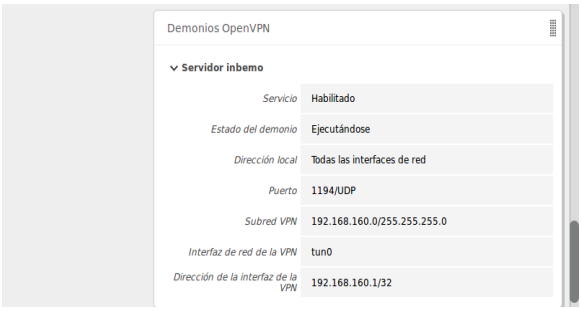


Figura 82. Verificar estado servidor.

5. Ahora hay que configurar el servidor, Seleccionamos el nombre del certificado del servidor que creamos en pasos anteriores

Figura 83. Evidencia configuración del servidor.

6. Luego configuramos el paquete que se debe descargar para la configuración del cliente y permitir la conexión VPN, En este apartado se hacer algunas configuraciones necesarias.
   - Seleccionar el tipo de cliente que se va a utilizar puede ser Linux, Windows o Mac OS.
   - Seleccionar el certificado que se creó para el cliente.
   - Estrategia de conexión se puede dejar la que viene por defecto Aleatorio.
   - La dirección del servidor.

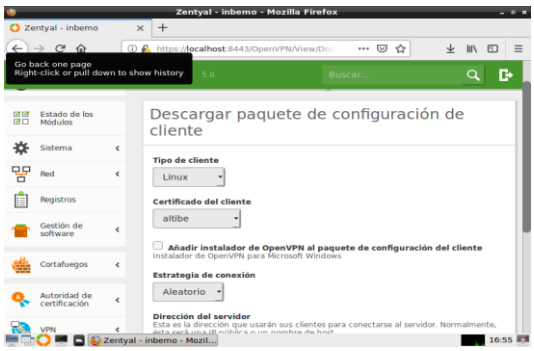


Figura 84. Configuración paquete configuración cliente.

7. Solo faltaría descargar el archivo de configuración del cliente. Después de esto copiamos estos archivos en una USB para utilizarlos una vez terminada la configuración del cliente.

8. Configuración del cliente que en este caso es un sistema operativo Linux Ubuntu. Entramos a la terminal para instalar el paquete Openvpn que el que nos permitirá hacer la conexión al servidor VPN.

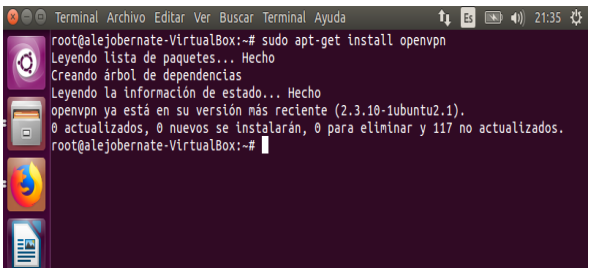


Figura 85. Instalación del paquete OpenVPN.

9. Copiamos la carpeta de configuración que se guardó en la usb en /etc/openvpn y la descomprimimos veremos los siguientes archivos.

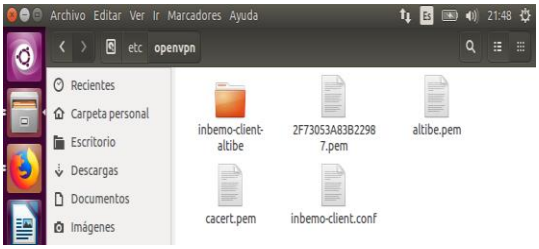


Figura 86. Vista de archivos de configuración.

10. Para realizar la conexión por interfaz gráfica tenemos que instalar.

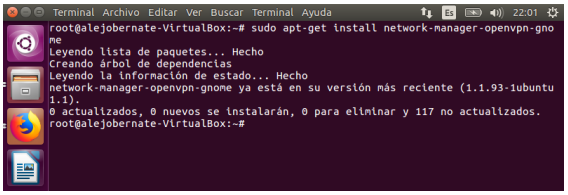


Figura 87. Instalación del paquete OpenVPN Gui

11. Entramos a conexiones de red y editar las conexiones y le damos clic en añadir elegimos el tipo de conexión y seleccionamos importar configuración VPN guardada que se encuentra al final.

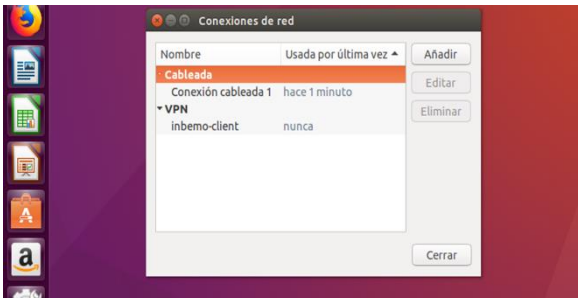


Figura 88. Configuración OpenVPN Gui.

12. Seleccionamos el archivo de configuración "Nombreseleccionado.conf", abrir y nos damos cuenta que se carga toda la configuración necesaria para la conexión y guardamos.

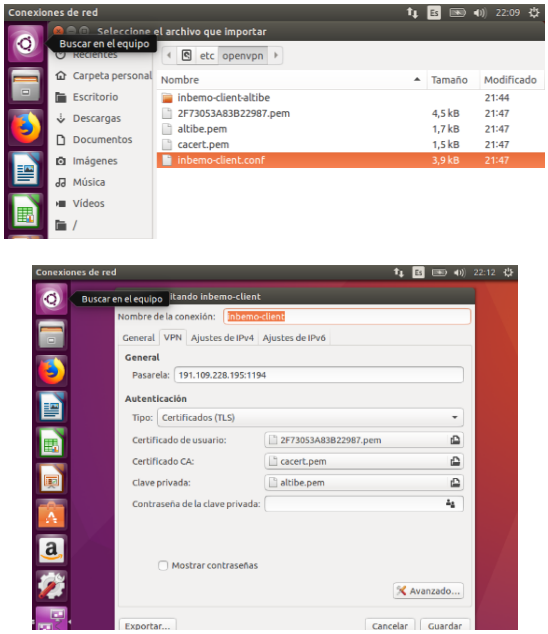


Figura 89. Vista de archivos de configuración.

13. Ahora vamos al panel de conexiones – conexiones VPN y seleccionamos la conexión que acabamos de crear y si todos los pasos están bien realizados ya tendremos: VPN que permita establecer un túnel privado de comunicación con una estación de trabajo GNU/Linux Ubuntu Desktop.

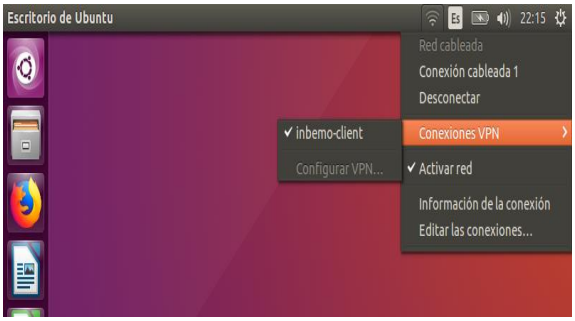


Figura 90. Comprobando conexión VPN.

5. Conclusiones.

Mediante el desarrollo de esta activad se nos permitió el correcto análisis e identificación del contenido del curso y sus temáticas, de acuerdo a las indicaciones dadas.

Se logra la correcta realización de los requerimientos planteados, enfocados en interpretar, identificar, aplicar y aprender en forma clara el Afinamiento de contenidos sobre GNU/Linux y el alistamiento del server para aplicar lo aprendido en el curso.

Al analizar la temática planteada se puede obtener un análisis que ha permitido generar un espacio crítico y de aplicación en este tipo de procesos.

Mediante el desarrollo de esta actividad se nos permitió la correcta implementación de las terminologías necesarias en este entorno.

6. REFERENCIAS

Módulo del curso de Diplomado De Profundización En Linux (Opción De Trabajo De Grado). UNAD. Bogotá. D.C. Consultado De: https://campus01.unad.edu.co/ecbti46/course/view.php?id=115

Lopez Sanches, M.J & Belle, S., & Auli, F. (2008). Sistema operativo GNU/Linux básico, ES: Universitat Oberta de Catalunya, Recuperado de http://hdl.handle.net/10609/189

Antonio, P. (2009). Administración de Sistemas GNU/LINUX, Fundación Código Libre Dominicano. Recuperado de http://www.mclibre.org/descargar/docs/manual-fcld/perpinan-gnu-linux-administracion-200307.pdf

Josep, J. E., & Remo, S. B. (2007). Administración avanzada de GNU/Linux. Universitat Oberta de Catalunya – UOC. Recuperado de http://hdl.handle.net/10609/226

Garcia, J. & Perramont, X. (2007), Aspectos avanzados de seguridad en redes. Universitat Oberta de Catalunya – UOC. Recuperado de http://hdl.handle.net/10609/204

Béjar, H. M. D. L. C. (2015). Selección, instalación, configuración y administración de los servidores de transferencia de archivos (UF1275). Madrid, ES: IC Editorial. Retrieved from http://bibliotecavirtual.unad.edu.co:2077/lib/unadsp/reader.action?ppg=150&docID=11148772&tm=1480301043772

Shah, S., & Soyinka, W. (2007). Manual de administración de Linux. México, D.F., MX: McGraw-Hill Interamericana. Retrieved from http://bibliotecavirtual.unad.edu.co:2077/lib/unadsp/reader.action?ppg=29&docID=10433920&tm=1480301276993

Diaz, G. Alzórriz, I. (2014). Procesos y herramientas par la seguridad de redes. Recuperado de.http://bibliotecavirtual.unad.edu.co:2460/lib/unadsp/reader.action?ppg=1&docID=3220062&tm=1513811615334