INSTALACIÓN Y CONFIGURACIÓN DE GNU/LINUX ZENTYAL SERVER 6.2, COMO SISTEMA OPERATIVO BASE PARA DISPONER DE SERVICIOS DE INFRAESTRUCTURA IT.

De Lima Rosado Elder
eodelimar@unadvirtual.edu.co
Pacheco Palomino Francy
flpachecop@unavirtual.edu.co
Aponza Cantoñi Ivan
icaponzac@unavirtual.edu.co
Pérez Díaz Elibeth
eperezd0@unavirtual.edu.co
Palomino Gerardo
glpalominon@unavirtual.edu.co

RESUMEN: *En el presente artículo se realiza la instalación y configuración de GNU/Linux Zentyal server 6.2, se definen la zona roja WAN internet, zona naranja DMZ desmilitarizada y zona verde LAN red interna local, de acuerdo a la Red administrable para acceder desde la estación de trabajo GNU/Linux al Zentyal Server, donde se configurarán los diferentes servicios de gestión de infraestructura IT, para dar solución a la problemática planteada. El trabajo contiene cinco temáticas, dentro de las cuales se devela la configuración detallada y puesta en marcha de los servicios: DHCP Server, DNS Server, Controlador de dominio, Proxy no transparente, Cortafuegos, File Server y Print Server y VPN.*

PALABRAS CLAVE: Zentyal Server, Infraestructura IT, Seguridad, Migración.

1 INTRODUCCIÓN

Este artículo se orienta a la configuración, administración y control de una distribución GNU/Linux basada en Ubuntu (Zentyal server), enfocada a la implementación de servicios de infraestructura IT de mayor nivel, donde se pondrán en marcha los diversos servicios solicitados y se validara su correcto funcionamiento como solución a la problemática en cuestión.

2 INSTALACIÓN SERVIDOR ZENTYAL

2.1 REQUISITOS MINIMOS PARA LA INSTALACIÓN

Para el Hardware estos requerimientos pueden variar de acuerdo de con los servicios que se vayan a implementar en el servidor, en términos generales se listan los requerimientos básicos que deben poseer los equipos donde se pretende instalar el servidor Zentyal, así:

- CPU Pentium 4.
- Memoria RAM 2G.
- Disco Duro 80G.
- Tarjeta de Red 2 o más.
- Arquitectura de 32 o 64 bits.

2.2 INSTALACIÓN Y CONFIGURACIÓN ZENTYAL SERVER 6.2

Se realiza la descarga de la imagen ISO del servidor Zentyal server versión 6.2 en el sitio oficial de Zentyal.

Figura 1. Sitio de descarga Zentyal server.

Una vez descargada la imagen ISO del sitio web oficial, se procede a crear la máquina virtual donde será montada la ISO para la instalación del sistema operativo de Zentyal server.

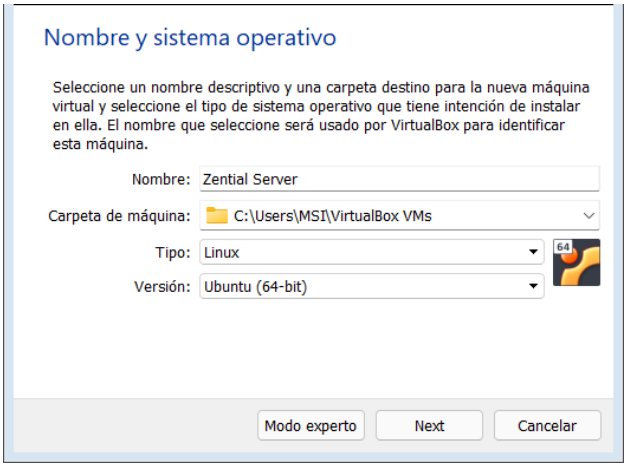

Figura 2. Instalación Zentyal server.

Instalación Sistema Operativo Zentyal server 6.2 finalizada.

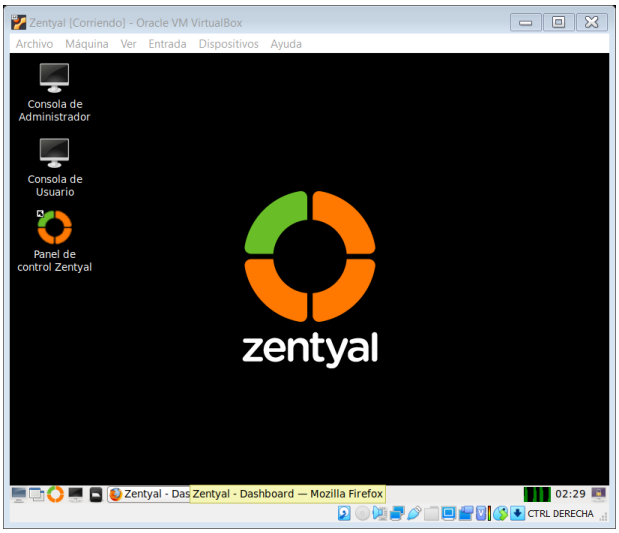

Figura 3. Instalación Zentyal server.

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

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

Se procede con la creación de los servicios controlador de dominio, DNS Server y DHCP Server en el servidor Zentyal.

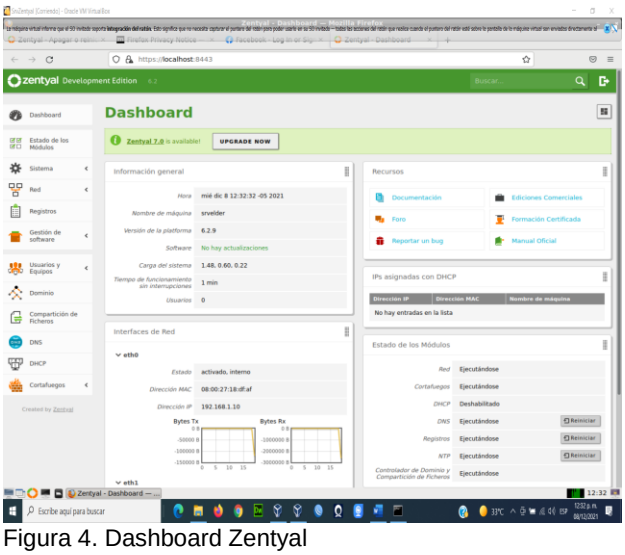

Figura 4. Dashboard Zentyal

Ahora en el panel izquierdo y en el menú DHCP, se activan los módulos.

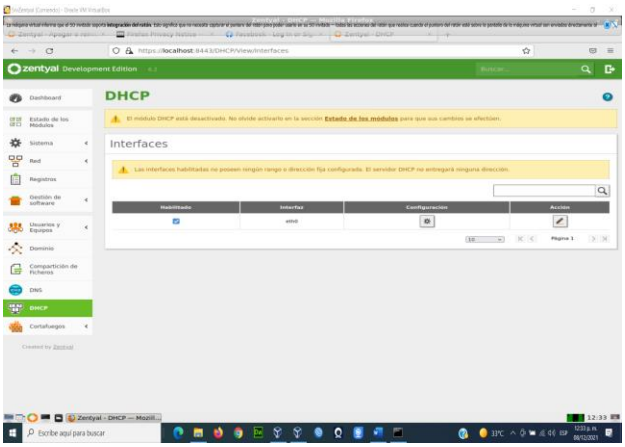

Figura 5. Configuración DHCP server

Configuración del servidor DHCP, primero se configura la puerta de enlace, de acuerdo a la asignada en el sistema operativo base.

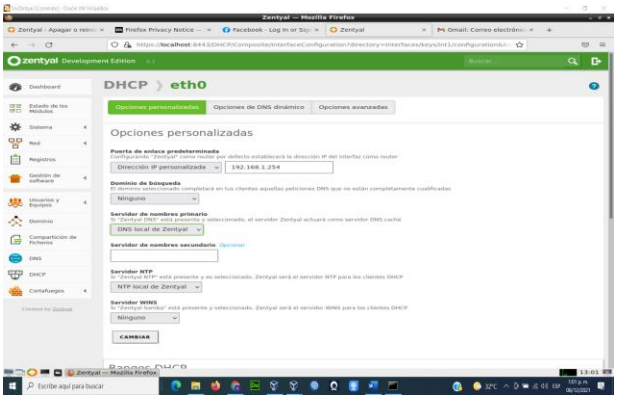

Figura 6. Configuración Dhcp server

Se crea la configuración del ámbito de red, esto va hacer el rango del IPS que va a proporcionar el DHCP server.

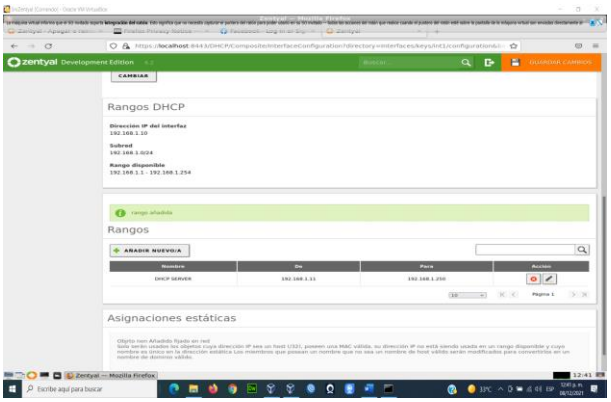

Figura 7. Configuración de ámbito de red

Ahora en la estación de trabajo GNU/Linux, en la terminal a través del comando ifconfig se valida la asignación de las direcciones IP por medio del servidor DHCP.

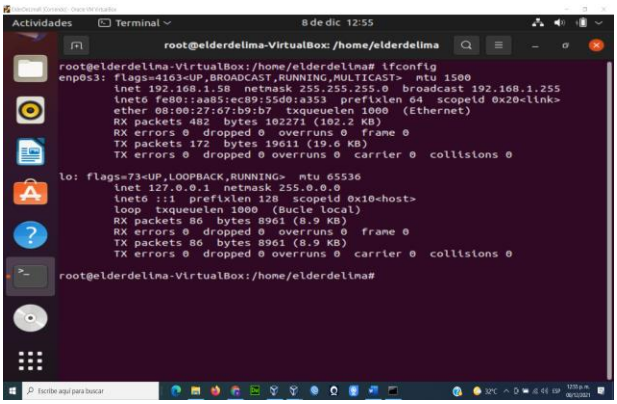

Figura 8. Comprobación de DHCP server en estación Linux

Se comprueba que el equipo está navegando haciendo un ping al dominio www.google.com, se evidencia que existe la comunicación con el dominio.

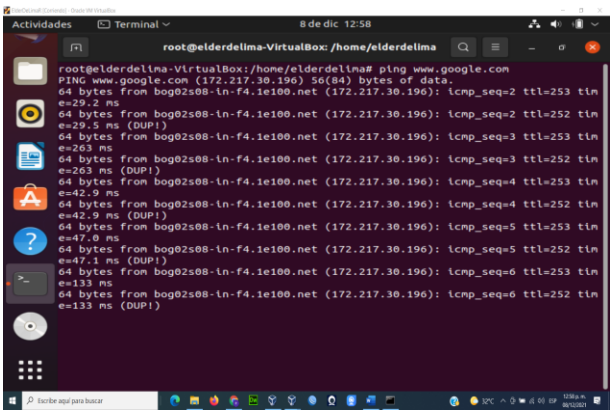

Figura 9. Ping a Google para comprobar la navegación.

Ahora en el Dashboard de Zentyal se puede observar como ya el DHCP ha asignado IP a la estación de trabajo.

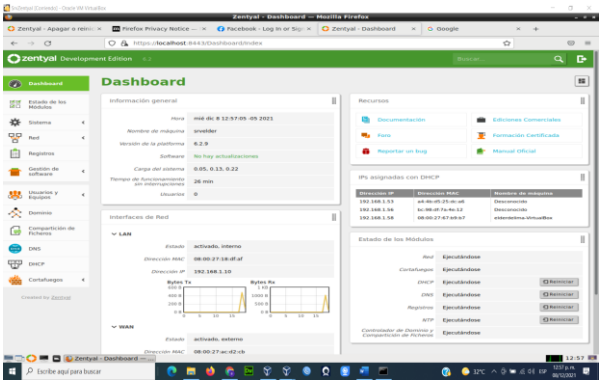

Figura 10. IPS asignadas en nuestra red

Luego en el panel izquierdo en el botón domino se comprueba si en la configuración inicial quedo instalado el dominio y se establece el dominio reino que para este caso es Dplinux.local; la función del servidor será controlar los dominios.

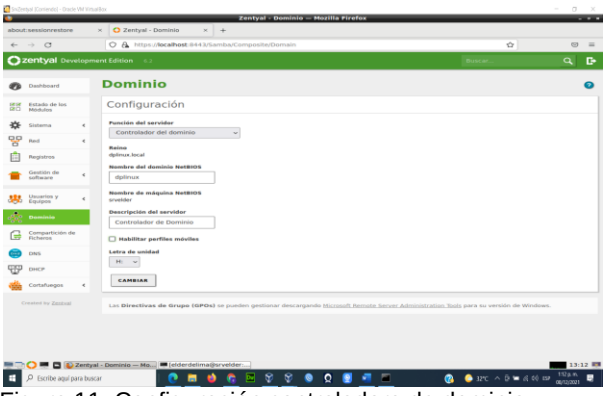

Figura 11. Configuración controladora de dominio

Ahora en el módulo DNS se ilustra como automáticamente se ha configurado el controlador de dominio, ya que este es quien va a hacer la resolución nombre de dominio de la red.

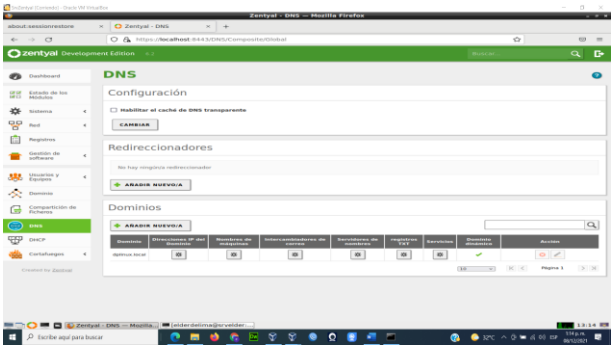

Figura 12 Configuración DNS

Luego en el módulo DHCP, opción de DNS dinámico se habilita las opciones del DNS dinámico para permitir la asignación de nombres de dominio a los clientes DHCP mediante la integración de los módulos de DHCP y DNS. De esta forma se facilita el reconocimiento de las máquinas presentes en la red por medio de un nombre de dominio único en lugar de las direcciones IP.

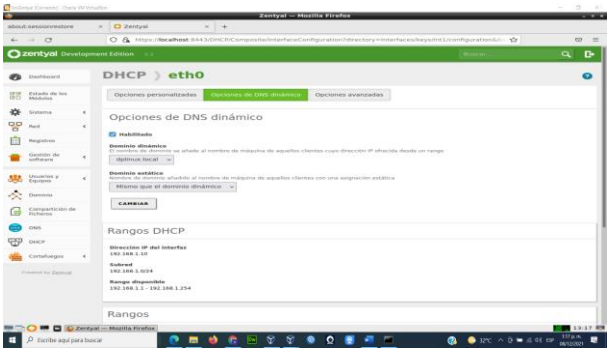

Figura 13. Configuración dns dinámico.

Creación del usuario controlador de dominio, Ahora en usuarios y equipos en el panel izquierdo, se da clic en users. Ahí muestra los usuarios que se han creado por defecto como lo son el Administrador y Guest. Luego se da clic en el icono + para añadir un nuevo usuario.

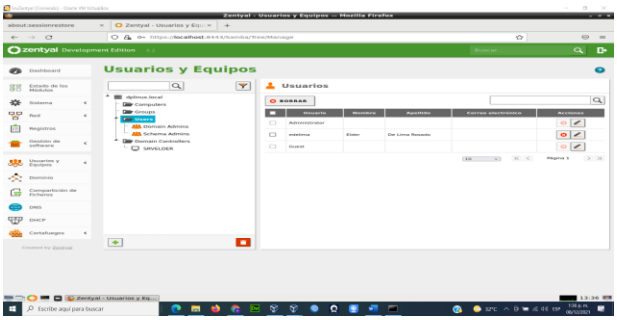

Figura 14. Creación de usuario nuevo controlador de dominio

En el equipo de la estación de trabajo se comprueba que se haya agregado con éxito al controlador de domino.

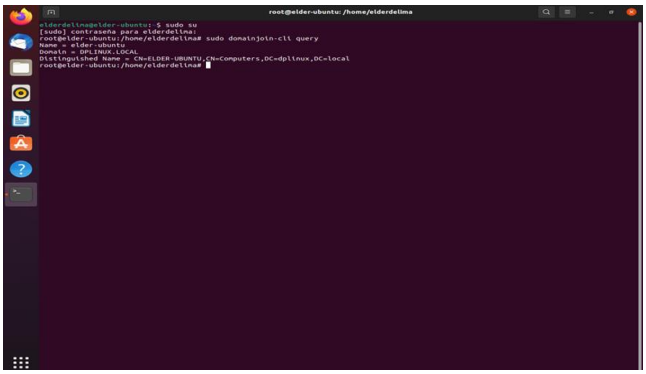

Figura 15. Estación Linux agregada al controlador de dominio

Luego en el servidor de controlador de dominio se evidencia las maquina asignada llamada ELDER-UBUNTO.

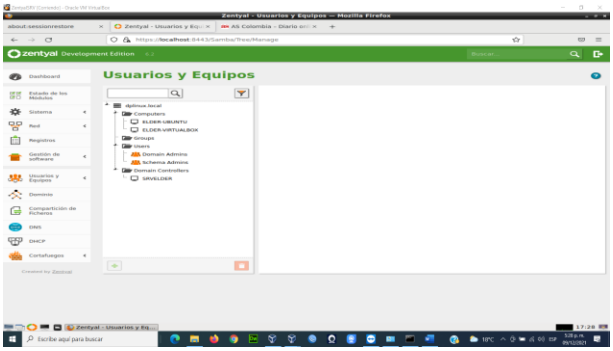

Figura 16. Estación reflejada en el controlador de dominio

Se reinicia el equipo luego se coloca el usuario administrator@dplinux.local y la contraseña asignada a este usuario.

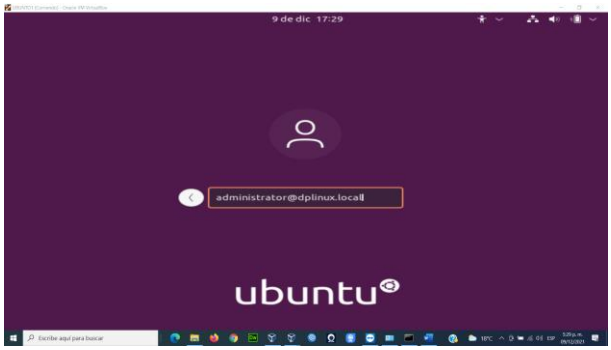

Figura 17. Ingresando con usuario de dominio a estación Linux.

En la terminal del cliente ubuntu se observa se puede observar el usuario administrador del controlador de dominio Dplinux.local.

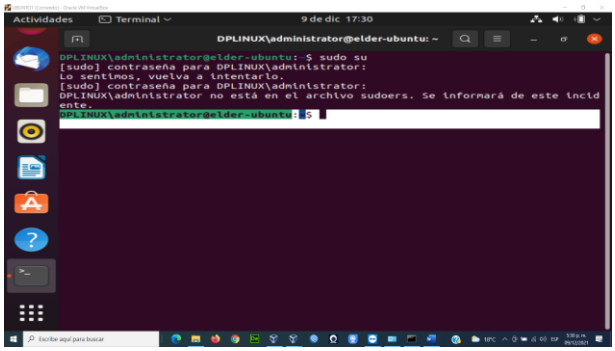

Figura 18. Verificando usuario en estación Linux.

Ahora se cambia de usuario para comprobar el usuario creado en el controlador de dominio que en este caso es edelima@dplinux.local con su contraseña asignada.

Figura 19. Nuevo inicio de sección con usuario creado

Ahora en la terminal de la estación de trabajo se puede ver que está logueado con el usuario del controlador de dominio Dplinux.local.

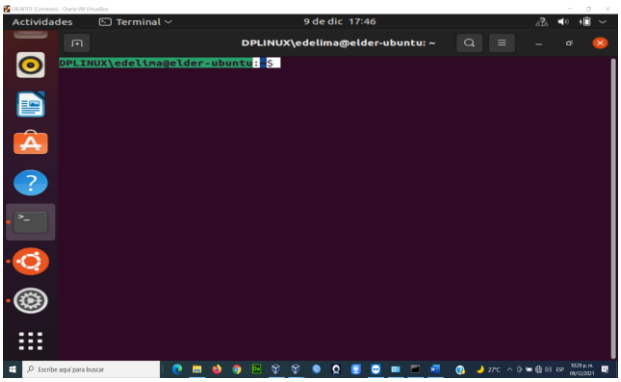

Figura 20. Usuario creado en estación Linux.

4 TEMÁTICA 2: PROXY NO TRANSPARENTE

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

Ingreso a Zentyal por medio del navegador con usuario y contraseña.

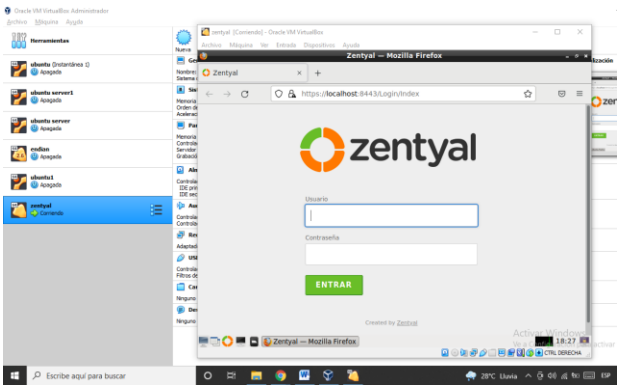

Figura 21. Ingreso a Zentyal.

En la instalación inicial de Zentyal se pueden ver los módulos y se selecciona el HTTP Proxy.

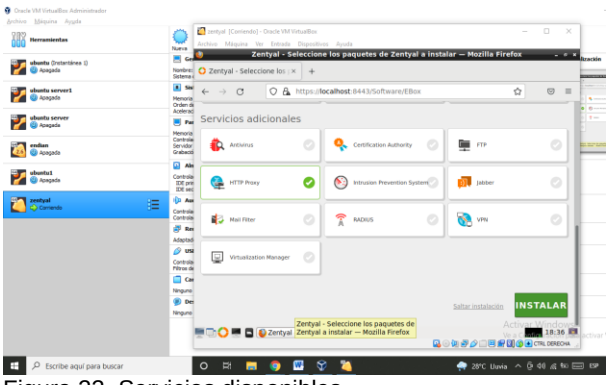

Figura 22. Servicios disponibles.

Se instalan los paquetes adicionales sugeridos por el modulo del proxy como lo son el Firewall, configuración de red.

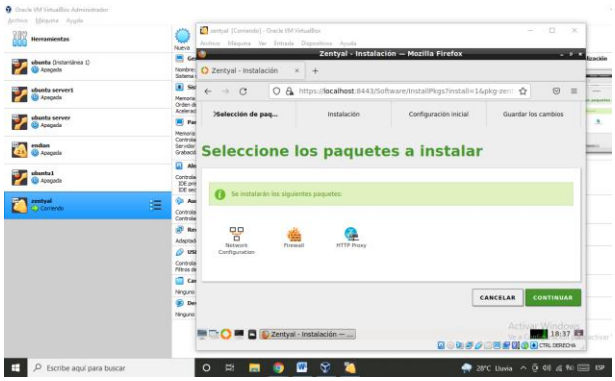

Figura 23. Seleccionar servicios.

Luego se espera que se instalen los paquetes.

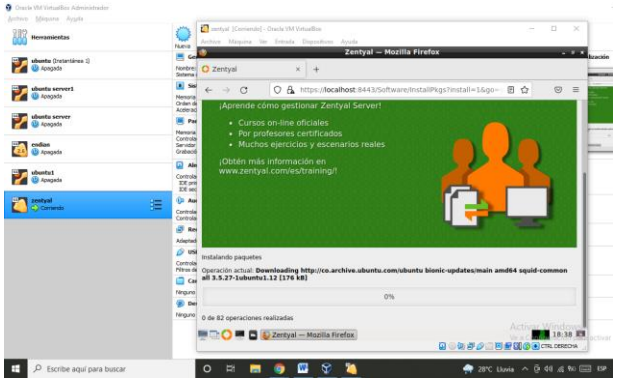

Figura 24. Instalación de paquetes.

En la opción estados de los módulos verificamos el estado de cada uno de los módulos y se procede a activarlos.

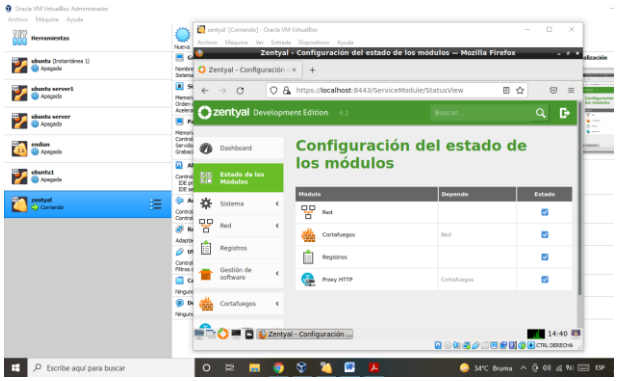

Figura 25. Estado de módulos.

En el modulo Proxy http -> Perfiles filtrados -> añadir nuevo, se crea el perfil de filtrado el cual se llamará “francy”.

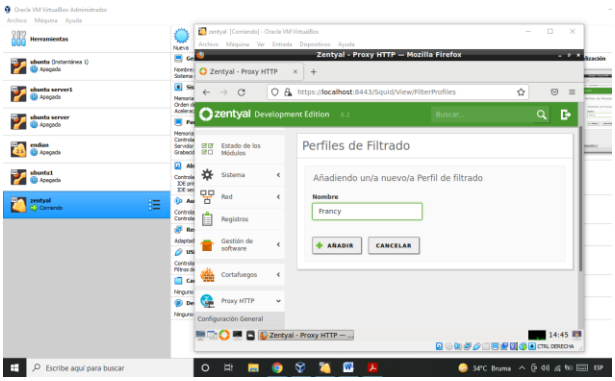

Figura 26. Creación de perfil.

Una vez creado el perfil le se da clic en configuración

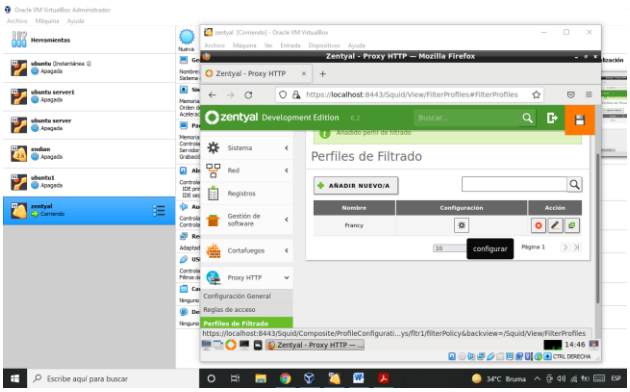

Figura 27. Configuración del perfil.

Estando en la configuración del perfil, se cambia el umbral de Deshabilitado a estricto.

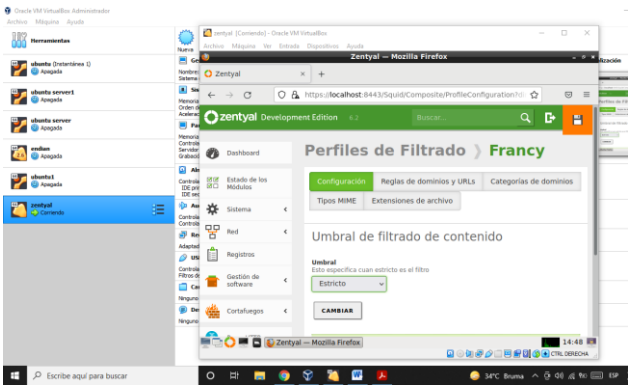

Figura 28. Cambio de estado Umbral.

Despues se dirije al modulo reglas de dominio y url, digita el nombre de la web que se va a bloquear y denegar el acceso de la misma.

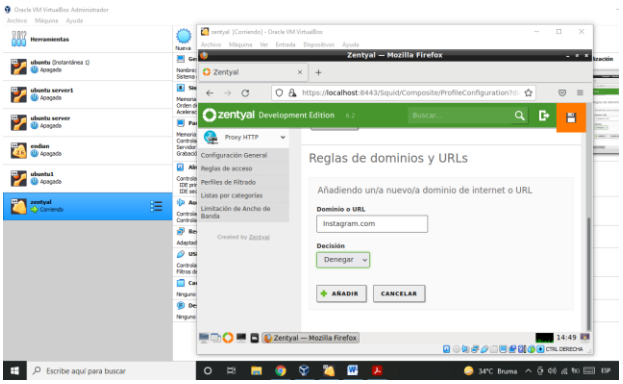

Figura 29. Creación de regla.

Ahora en la configuracion general del modulo proxy http se cambia el puerto a 1230 a travez del cual se va a filtrar todo el trafico de salida de acuerdo a los solicitado.

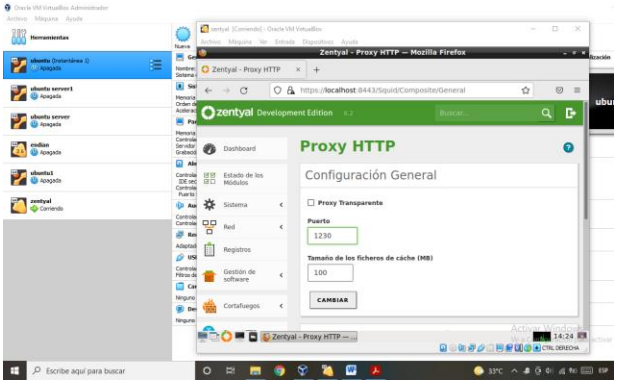

Figura 30. Configuración del puerto.

Ahora se añadir una regla de acceso al perfil creado anteriormente.

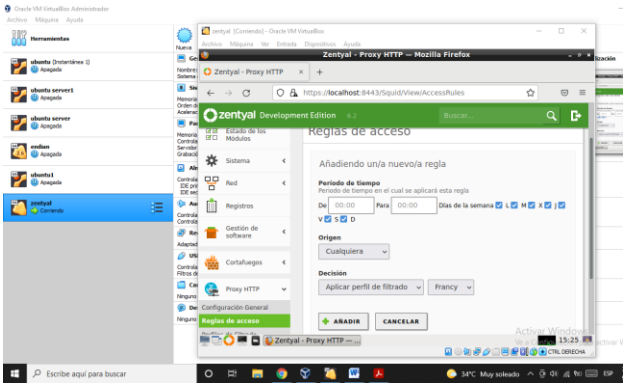

Figura 31. Configuración regla de acceso.

Luego se iniciar el equipo de la estación de trabajo GNU/Linux.

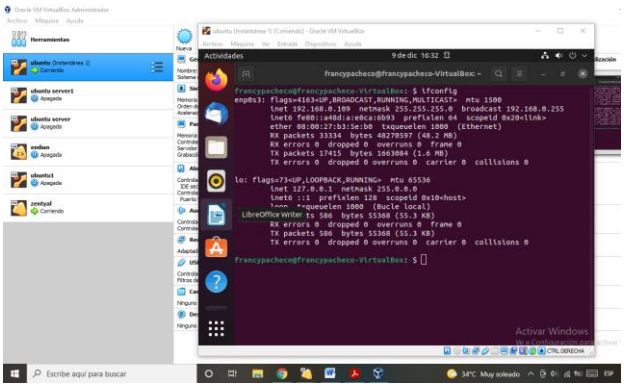

Figura 32. Ubuntu desktop.

Ahora en el navegador de la estacion de trabajo GNU/Linux, se cambia la configuracion del proxy se ingresa la dirección IP de zentyal y el puerto 1230 configurado para filtrar las salidas.

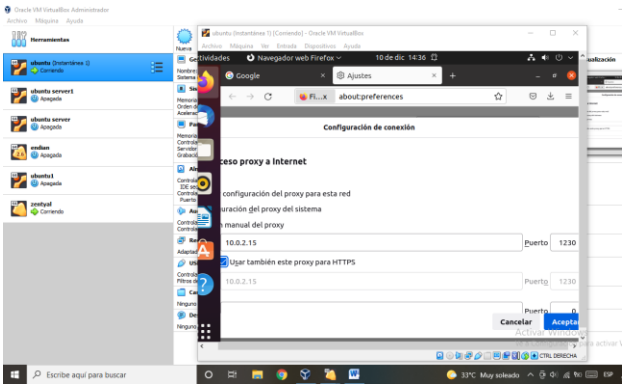

Figura 33. Configurar proxy Ubuntu.

Se ingresa al sitio web Facebook.com para validar que el proxy este denegando el acceso a la estación de trabajo GNU/Linux, como se observa el proxy esta denegando el acceso a a este sitio, evidenciandose que que la reglas quedaron bien configuradas.

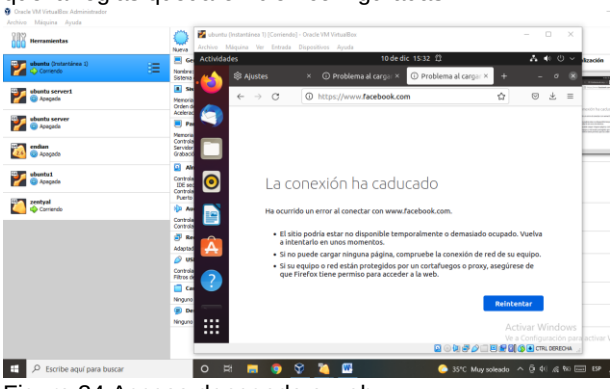

Figura 34 Acceso denegado a web.

Para finalizar se ingresa a la configuracion del navegador y se retira las configuración del proxy realizada en la estación de trabajo GNU/Linux.

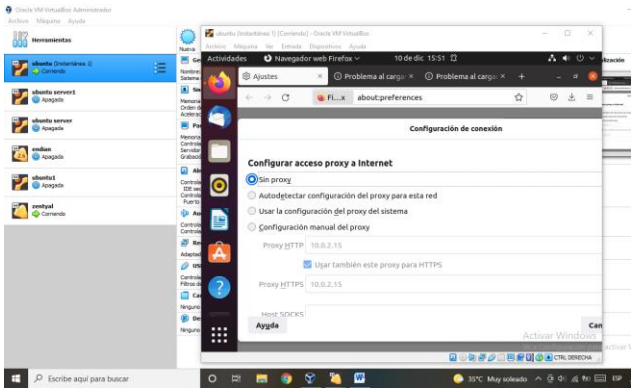

Figura 35. Retirar configuración proxy.

Una vez se retiran las configuraciones del proxy realizadas en el navegador del aestación de trabajo, se Valida que el equipo de la estación de trabajo pueda ingresar al sitio web de Facebook.com.

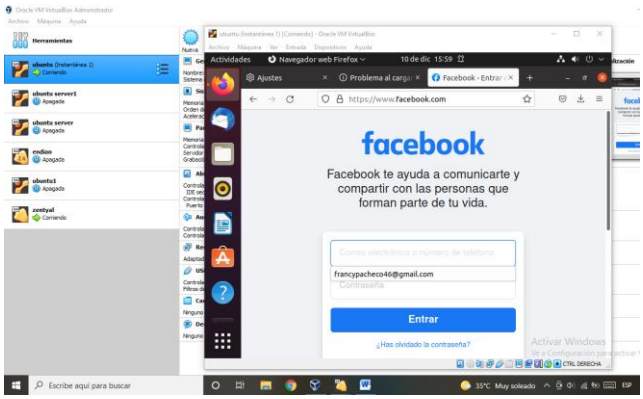

Figura 36. Ingreso Facebook.

5 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.

Se procede a seleccionar los paquetes a instalar para la configuración del módulo de cortafuego como son DHCP y Firewall.

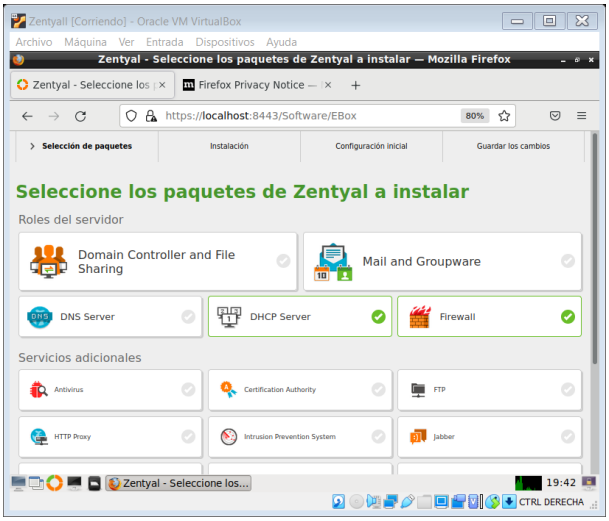

Figura 37. Selección de paquetes.

El modulo instala paquetes adicionales como son Configuración de red, DNS server, NTP service y el Domain controller**.**

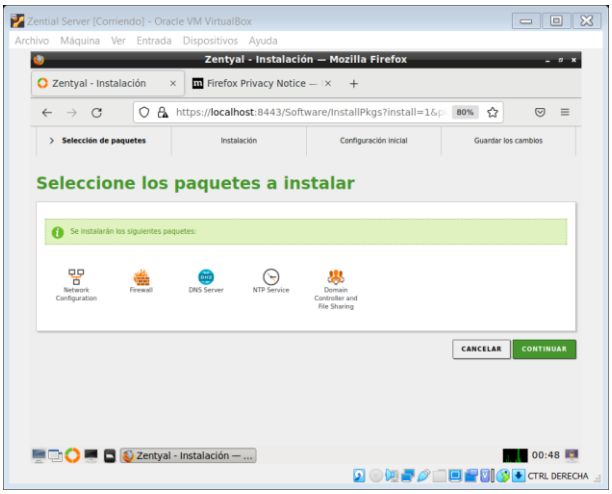

Figura 38. Paquetes adicionales.

Luego se configura las interfaces de red eth0 método DHCP, externa WAN.

Figura 39. Interfaces de red eth0 DHCP

Seguidamente se configura la interface de red eth1 como red interna, método estático asignando la IP 192.168.200.3.

Figura 40. Interfaces de red eth1 Static.

Luego en el módulo DHCP se configura un rangos de red para que el servidor asigne las direcciones IP a los equipos de la red local.

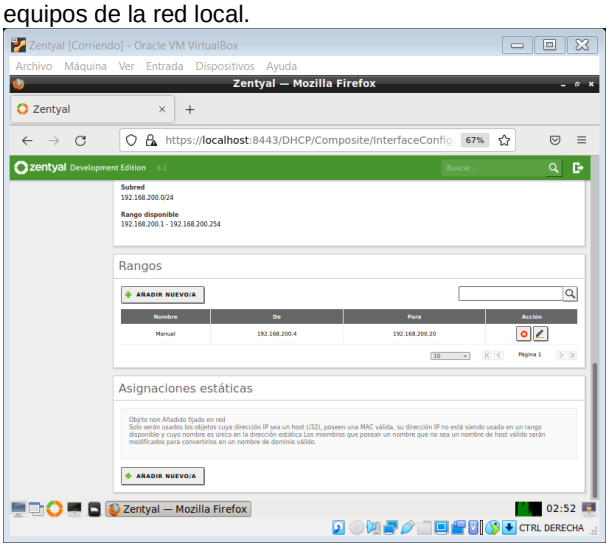

Figura 41. Asignación rango de red.

Una vez instalado y configurado las interfaces de red y el rango de red en el módulo DHCP, en el Dashboard del servidor Zentyal se puede observar las interfaces de red configuradas y las IP asignadas por DHCP y el estado de los módulos instalados.

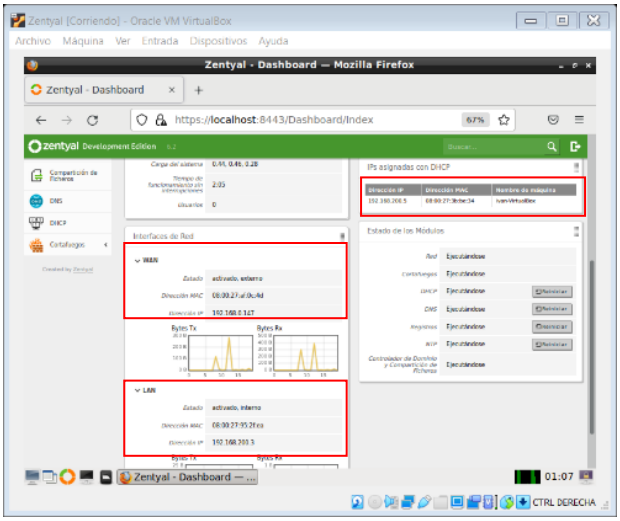

Figura 42. Dashboard Zentyal Server.

Se procede a crear un objeto de red llamado “FirewallDPLinux” y dentro de este un miembro denominado “Linux”, al cual se le asigna un rango de direcciones IP de acuerdo al segmento de red interna del servidor, que se utilizaran para aplicar las restricciones.

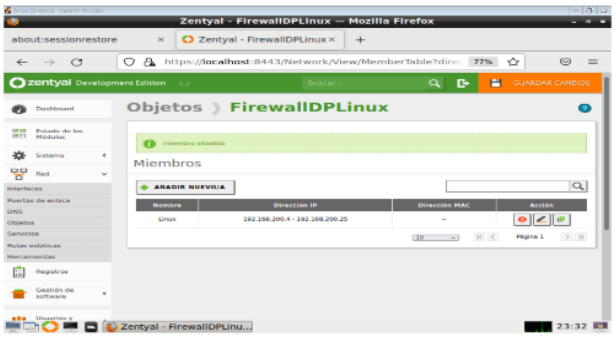

Figura 43. Creación objeto y miembros de red.

Para la configuración de la regla para restringir la redes social Facebook se ingresa desde la estación de trabajo GNU/Linux al navegador para validar que se pueda navegar en el sitio web.

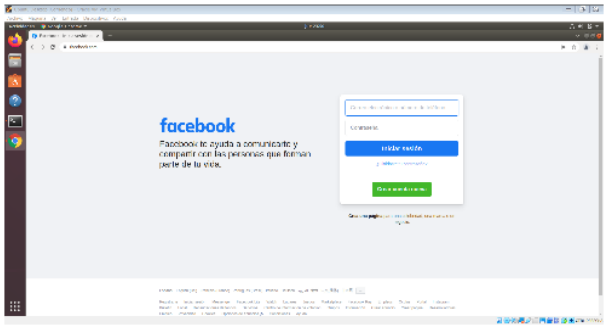

Figura 44. Ingreso sitio web Facebook

Para verificar la comunicación y la dirección IP de Facebook se realiza un ping al dominio www.facebook.com.

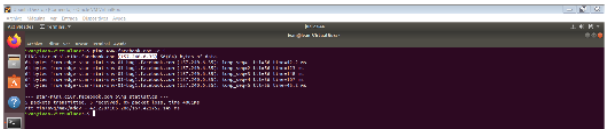

Figura 45. Ping Facebook.com

Ahora para crear las reglas de restricción de acceso a las redes social Facebook, se ubica el módulo de cortafuegos opción Filtrado de paquetes, se observa las secciones del Firewall, luego en la sección Regla de filtrado para las redes internas.

Figura 46. Modulo cortafuego filtrado de paquetes.

Se ingresa la información indicando la decisión “DENEGAR”, en el origen se selecciona el objeto de origen creado anteriormente “FirewallDPLinux”, en el destino se ingresa la dirección IP de Facebook consultada a través del ping realizado al dominio “157.240.6.35/32”, en servicio se selecciona cualquier servicio y en la descripción se coloca Bloqueando redes social Facebook.

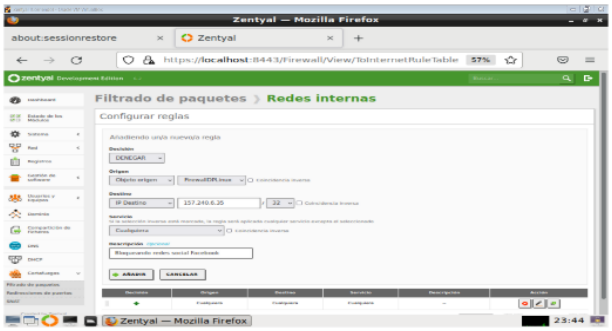

Figura 47. Creación regla de filtrado de paquete.

Ahora ya se han creado todas las Reglas restringiendo el acceso a las redes social y sitios de entretenimiento.

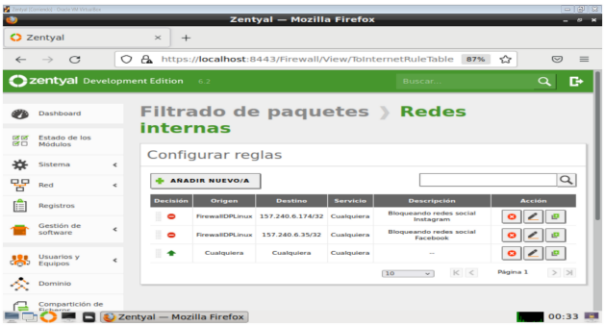

Figura 48. Listado Reglas creadas.

Para validar que la regla haya quedado bien montada y estén funcionando, se ingresa nuevamente a la estación de trabajo GNU/Linux, luego en el navegador se intenta acceder a las redes social Facebook y como se observa el cortafuego está restringiendo el acceso, lo que indica que las reglas quedaron bien configuras y está cumpliendo la función para cual fue creada.

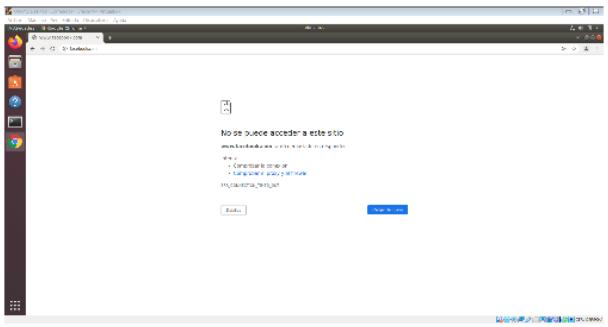

Figura 49. Validación funcionamiento regla creada.

Finalmente, desde la estación de trabajo GNU/Linux se ingresa a una dirección o dominio distinto a las restringidas para validar que el cortafuego esté funcionando correctamente, como se evidencia permite el acceso sin problemas a los otros dominios.

Figura 49. Validación navegación en otros dominios.

.

6 TEMÁMICA 4: FILE SERVER Y PRINT SERVER

Producto esperado: Implementación y configuración detallada del acceso de una estación de trabajo GNU/Linux a través del controlador de dominio LDAP a los servicios de carpetas compartidas e impresoras**.**

Inicialmente se instala el servidor Zentyal server 6,2 en una máquina virtual, para el caso se usa VirtualBox. Una vez instalado el servidor automáticamente se visualiza en el navegador Firefox, el login donde solicita ingresar el usuario y contraseña asignados en la instalación.

Figura 50: instalación de Zentyal

Posteriormente se realiza la configuración inicial de instalación, módulos necesarios del controlador de dominio dentro del servidor, seguidamente se selecciona el paquete Domain Controller and File Sharing.

Zentyal sugiere módulos adicionales necesarios para la instalación como controlador de dominio.

Figura 51: Configuración inicial de Zentyal

El proceso de instalación requiere configuración de las redes, la primera como Interna y la segunda como Externa.

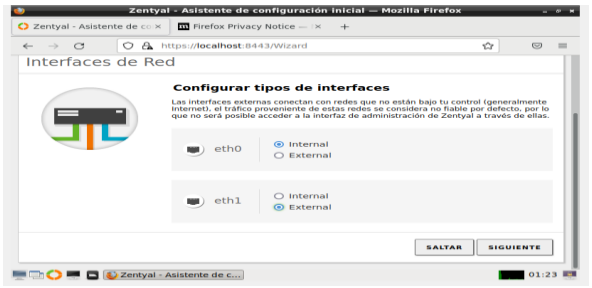

Figura 52: Configuración de redes Zentyal

El adaptador de red Interna con DHCP. La Externa con una IP estática, asignada en la configuración para comunicación entre los equipos en red.

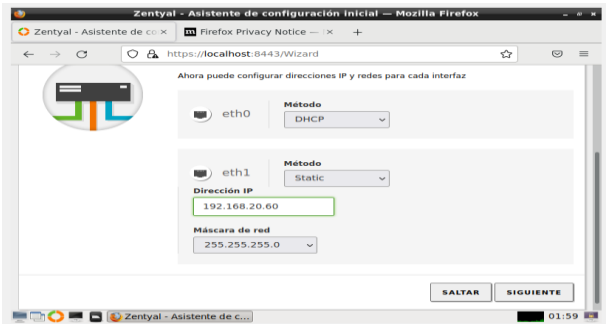

Figura 53: Configuración de IP en Zentyal

Se abre la terminal de Zentyal para validar por medio del comando ifconfig que se tenga conexión a internet y visualizar la configuración de las redes.

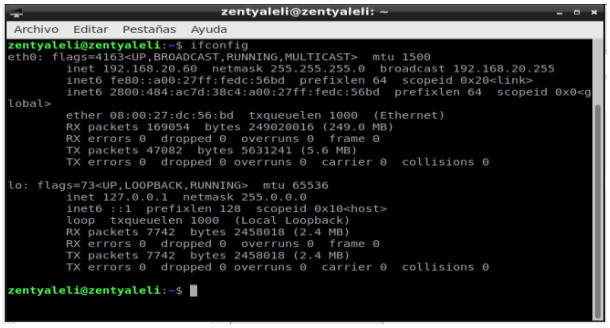

Figura 54: Terminal de Zentyal

Ahora se selecciona el tipo de servidor (servidor stand-alone) y se asigna el nombre del dominio para su posterior uso en la conexión a través de LDAP.

Figura 55: Configuración de servidor Zentyal

Se ingresa al menú usuarios y equipos, en configuración de LDAP se visualiza la información en el bloque inicial.

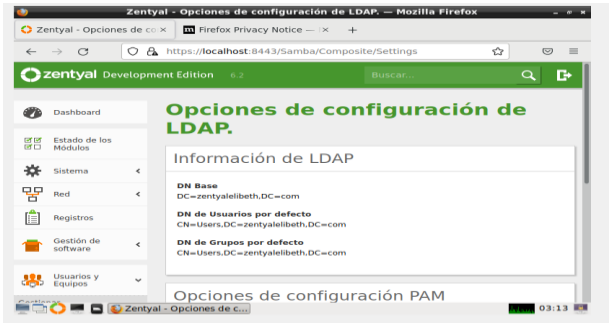

Figura 56: Opciones de configuración de LDAP de Zentyal

En el mismo menú usuarios y equipos > opción gestionar se visualiza el árbol de LDAP, donde se gestiona los atributos de los nodos, agregar usuarios, grupos.

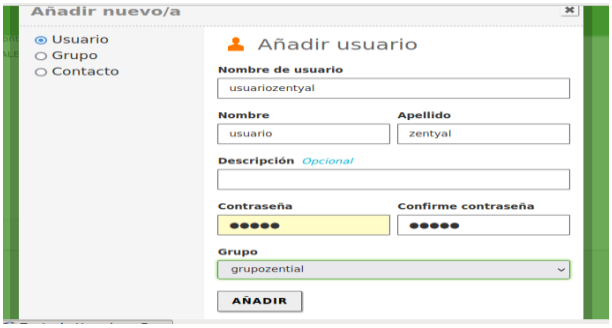

Figura 57: Se añade un nuevo usuario a árbol

Desde el menú compartición de ficheros se crea un directorio compartido, habilitando el recurso y asignado la ruta.

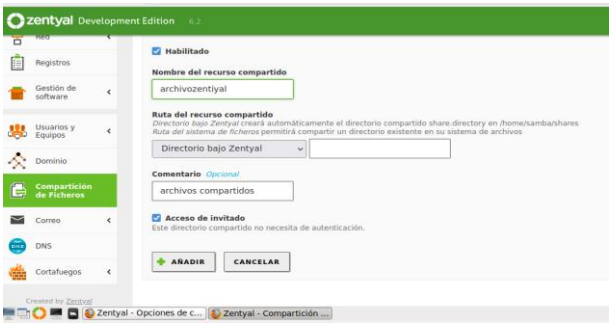

Figura 58: Creación de fichero compartido

Desde el control de acceso se añade a un nuevo ACL con el grupo o usuario creado y dando permiso con administrador

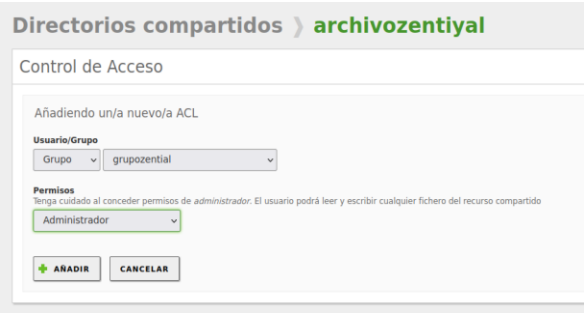

Figura 59. Control se acceso a directorios compartidos

ESTACIÓN DE TRABAJO GNU/LINUX UBUNTU

En la estación de trabajo GNU/Linux se configura la red para que se conecten con la dirección IP Fija asignada al servidor.

Figura 60. Control se acceso a directorios compartidos

Se abre la terminal de la estación de trabajo GNU/Linux y se descarga el paquete pblis-open en su version 9.1.0 para que la maquina se conecte con el domino, se intala para su posterior confirguración .

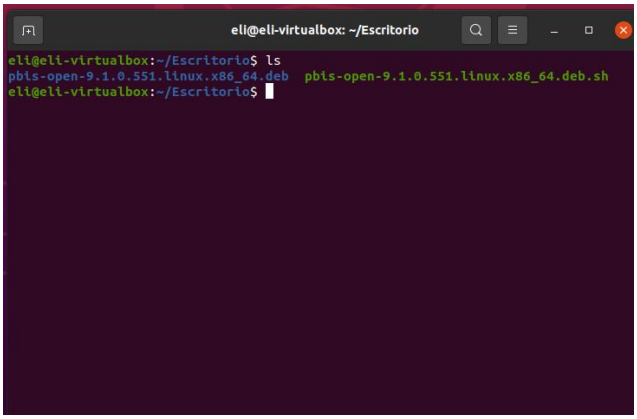

Figura 61: Instalación de paquetes en terminal Ubuntu.

Se realiza la configuración usando el comando /opt/pbis/bin/domainjoin-cli join –disable ssh ZENTYALUNAD.LAN eliperez, estos nos configura DC.

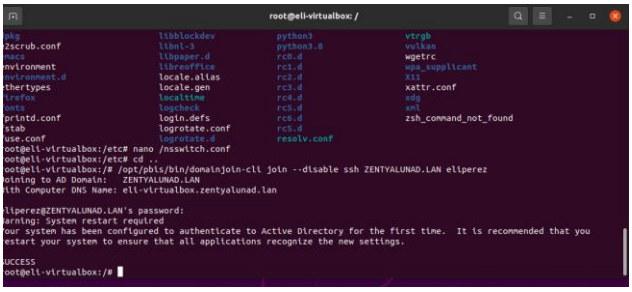

Figura 62. Configuración de protocolo de conexión.

Posterior a la configuración del controlador de dominio, se ingresa a Equipo en los archivos y se agrega la dirección en la barra de búsqueda: smb:/192.168.1.2 y muestra la carpeta compartida del servidor Zentyal.

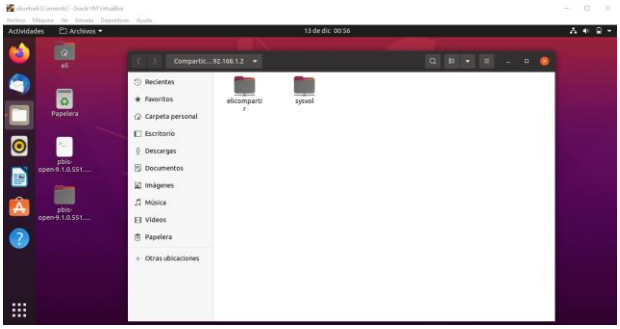

Figura 63. Carpetas compartidas

Para agregar una impresora en Zentyal, se abre el nevegador y se escribe la direccioón http://localhost:632/. La cual abre una pagina de cups, desde la pestaña administrador y se adiciona una impresora.

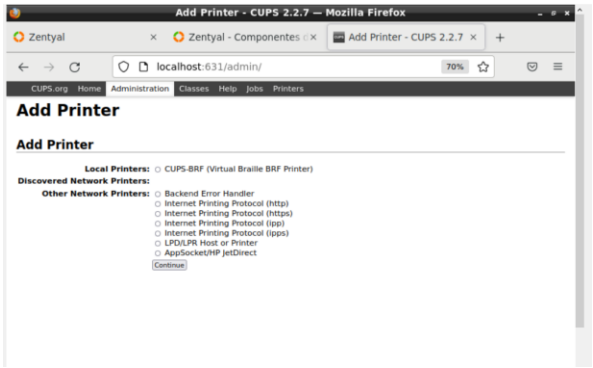

Figura 64. Instalación de impresora en Zentyal.

Se agrega y configura la impresora en Zentyal para compartirla con la estación de trabajo GNU/Linux.

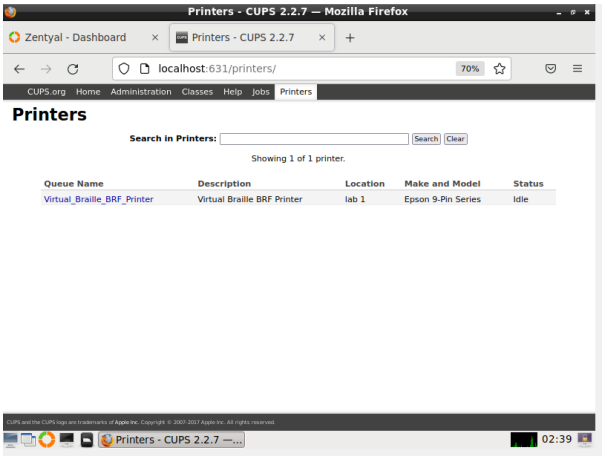

Figura 65. Configuración de impresora en Zentyal.

Desde la estación de trabajo se busca y configura la impresora para que se pueda imprimir documentos.

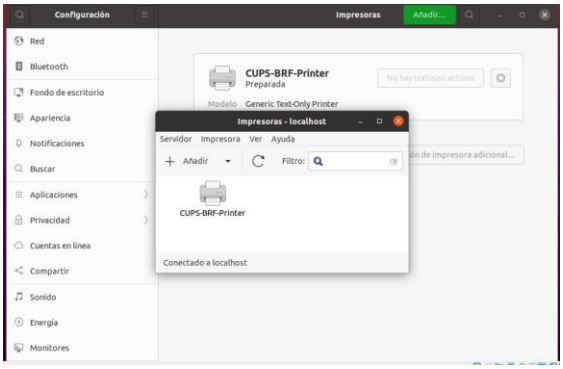

Figura 66. Ubicación de la Impresora desde la estación de trabajo Ubuntu.

7 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. Se debe evidenciar el ingreso a algún contenido o aplicación de la estación de trabajo.

Se procede a seleccionar los paquetes a instalar para la configuración del módulo VPN.

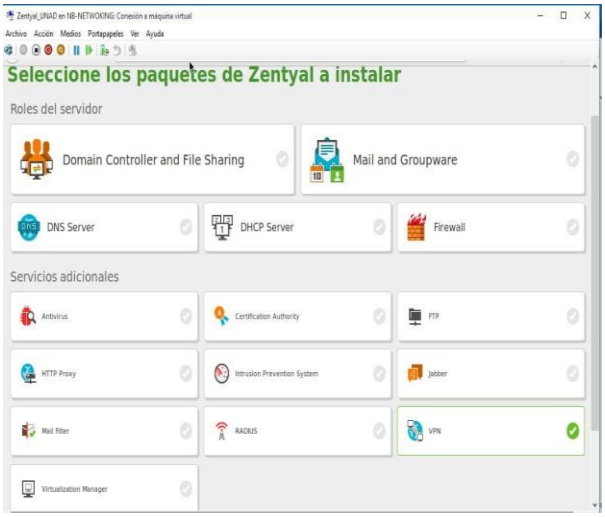

Figura 67. Selección de paquetes.

El modulo sugiere instalar paquetes adicionales como son Configuración de red, Firewall, Certificación Authority.

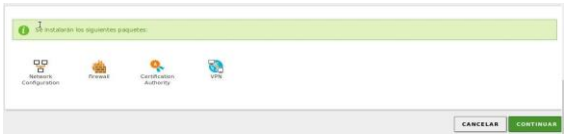

Figura 68. Paquetes adicionales.

Luego se crea el servidor VPN.

Figura 69. Creación el VPN.

Se descarga la configuración del servidor.

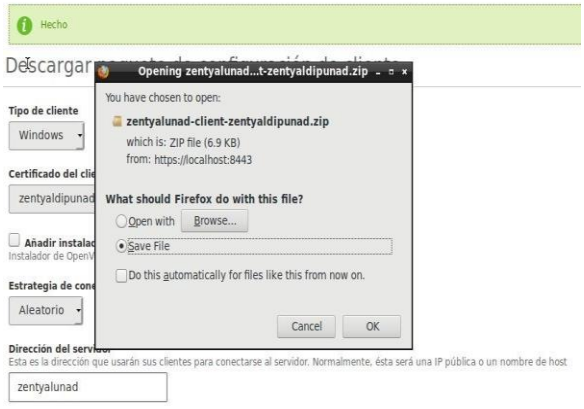

Figura 70. Descarga servidor.

Se procede a crear el certificado que permitirá a los clientes realizar la conexión al servidor VPN.

Figura 64. Servidor VPN.

Luego en el módulo de autoridad de certificación se procede a realizar la creación del certificado.

Figura 71. Creación certificada de la autoridad de certificación.

Ahora se observa el listado de certificados creados.

Figura 66. Listado certificados creados.

Se descarga el certificado a aplicar en el cliente VPN a conectar, en el equipo cliente donde se aplicará luego de instalado el OpenVPN como aplicación de conexión.

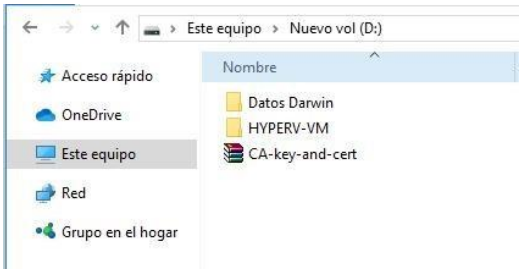

Figura 72. Archivos Descargados.

Ahora en la página oficial OpenVPN se procede a descargar el cliente VPN.

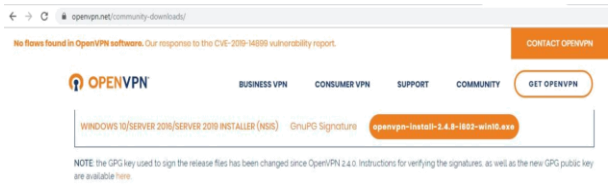

Figura 68. Sitio oficial OpenVPN.

Se inicia el asistente de instalación, y se siguen los pasos.

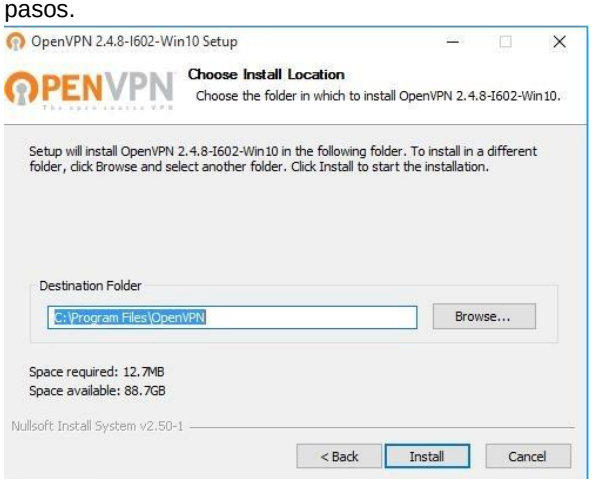

Figura 73. Instalación OpenVPN.

Al instalarse se procede a importar el archivo descargados, (el certificado) que permitirá establecer la conexión VPN, igualmente notifica que el archivo se importa correctamente.

Figura 74. Instalación satisfactoria.

Se procede a realizar la conexión.

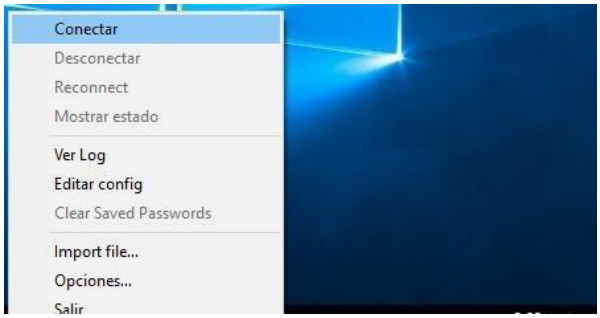

Figura 75. Conexión.

Establecida la conexión se procede a realizar la prueba, en este caso se valida la dirección IP que tiene el servidor 192.168.43.96.

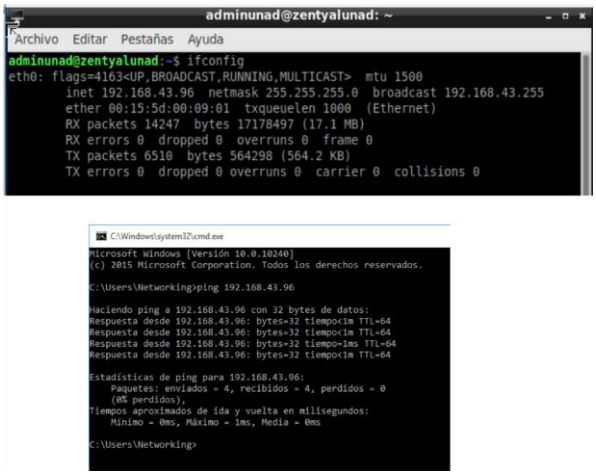

Figura 76. Validación de conexión.

Finalmente se valida que dentro del Zentyal aparezca la conexión activa de la VPN establecida.

Figura 77. Validación conexión activa.

8 CONCLUSIÓN

Teniendo en cuenta los diferentes conceptos, técnicos y teóricos se logra instalar, configurar y poner en marcha la infraestructura tecnológica que permitió dar respuesta a la problemática de migración, la cual se realizó bajo GNU/Linux Zentyal Server version 6.2, como sistema operativo base para disponer de los servicios de Infraestructura IT, en el cual se implementaron los servicios DHCP Server, DNS Server, Controlador de dominio, Proxy no transparente, Cortafuegos, File Server y Print Server y VPN.

Para el registro acceso y control desde de una estación de trabajo GNU/Linux a Zentyal server, a través del usuario y contraseña creado; se implementó un servicio de conectividad a Internet a través de un proxy que filtra todas las salida por medio del puerto 1230; se configuraron las reglas de filtrado para la restricción de la apertura de sitios o portales Web de entretenimiento y redes sociales; se configuro un controlador de dominio LDAP para los servicios de carpetas compartidas e impresoras; se creó una VPN que permite establecer un túnel privado de comunicación con la estación de trabajo GNU/Linux.

Se logra validar el correcto funcionamiento de cada uno de los servicios implementados como solución a los requerimientos de infraestructura tecnológica para el proceso de migración de la empresa.

9 REFERENCIAS

[1] Zentyal. (2018). Servicio de resolución de nombres de dominio (DNS). Recuperado de https://doc.zentyal.org/es/dns.html#configuracion-de-un-servidor-dns-autoritario-con-zentyal

[2] (2018). Servicio de configuración de red (DHCP). Recuperado de https://doc.zentyal.org/es/dhcp.html

[3] Zentyal. (2018). Configuración general del Proxy HTTP Recuperado de https://doc.zentyal.org/es/proxy.html.

[4] Zentyal S.L. (2018). Configuración de un cortafuego con Zentyal. Recuperado de: https://doc.zentyal.org/6.2/es/firewall.html#configuracion-de-un-cortafuegos-con-zentyal.

[5] *Zentyal. (2018). Servicio de redes privadas virtuales (VPN) con OpenVPN. Recuperado de https://doc.zentyal.org/es/vpn.html*

[6] Zentyal S.L. (2018). Instalación. Recuperado de: https://doc.zentyal.org/6.2/es/installation.html