ZENTYAL COMO SERVIDOR DE INFRAESTRUCTURA

Marlyn Sneidy Giraldo Múnera
e-mail: msgiraldomu@unadvirtual.edu.co
César Augusto Mejía Osorio
e-mail: camejiaos@unadvirtual.edu.co
Luis Felipe Cuervo Cardona
e-mail: fcuervo71@gmail.com
Jaime Alexis Betancurt Londoño
e-mail: jabetancurtl@unadvirtual.edu.co
Diego Fernando Campos Murillo
e-mail: dfcamposm@unadvirtual.edu.co

RESUMEN: *Zentyal es un servidor desarrollado especialmente para PyMES como alternativa de código abierto a Microsoft Windows Server. Dentro de sus características está su facilidad de instalación, configuración y la sencillez de su administración. Aprovechando estas ventajas se realizó la configuración de los servicios DHCP Server, DNS Server y controlador de dominio. Se implementó un proxy para control de acceso a internet desde Zentyal, filtrando la salida a través del puerto 830. Se configuró Zentyal como firewall para restringir el acceso a sitios web de entretenimiento y redes sociales. Se configuró el acceso a través de un controlador de dominio LDAP a los servicios de carpetas compartidas e impresoras y se creó una VPN para establecer un túnel privado de comunicación con una estación de trabajo. Los servicios mencionados anteriormente fueron implementados con éxito y sus pruebas se realizaron en estaciones de trabajo GNU/Linux Debian 10.*

PALABRAS CLAVE: Cortafuegos, CUPS, Debian, DHCP, DNS, Dominio, File Server, Firewall, LDPA, Print Server, Proxy, SAMBA, Servidor, VPN, Zentyal.

1 INTRODUCCIÓN

Zentyal es una distribución de Linux adaptada como servidor, gracias a que está basado en Ubuntu (actualmente basado en 18.04.3 LTS), en muy sencillo de administrar, pues integra su propio panel de forma web. Su desarrollo busca generar ser una alternativa real a Windows Server o a Novell Suite Small Business Edition, ya que incluye todos los servicios necesarios para abordar la gestión y administración de los servicios esenciales para arrancar una pequeña o mediana empresa, tales como gestión de red, servidor de correo, administración de comunicaciones, compartición de recursos y trabajo en grupo, gestión centralizada de usuarios e incluso servir como autoridad de certificación para una red local [5].

A continuación, se muestra el paso a paso de la instalación de Zentyal como servidor, además de su configuración inicial. Como se montaron los servicios DHCP y DNS, servidor de impresoras, controlador de dominio, proxy para control de acceso a internet, firewall para restringir el acceso a sitios web y VPN para lo cual se usó la versión 6.2.

2 INSTALACIÓN ZENTYAL 6.2

Se debió configurar dos tarjetas de red para la instalación del sistema operativo. Se configuró además el adaptador 1 como adaptador puente.

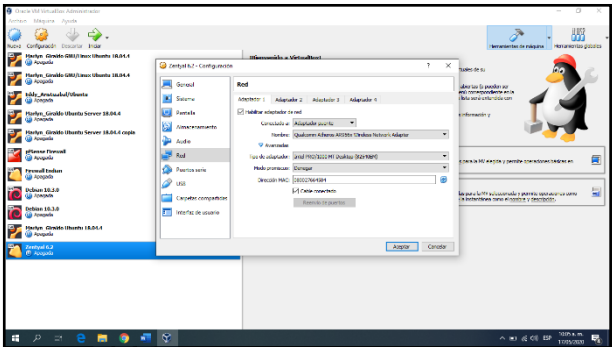

Figura 1 Configuración de adaptador 1

Se configuró el adaptador 2 como red interna donde se procedió a establecer la red LAN, la cual se nombró como Zentyal_LAN.

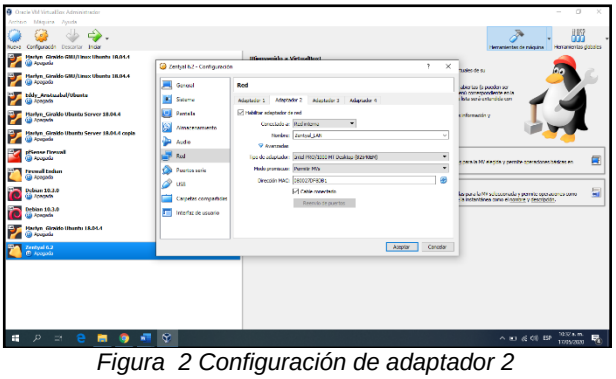

Figura 2 Configuración de adaptador 2

Se seleccionó la opción de instalación de Zentyal 6.2. y se borró todo el disco, luego se configuró la ubicación e idiomas.

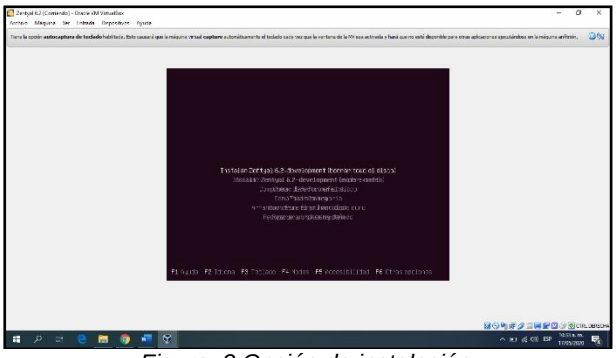

Figura 3 Opción de instalación

Se seleccionó la interfaz de red primaria para el sistema operativo.

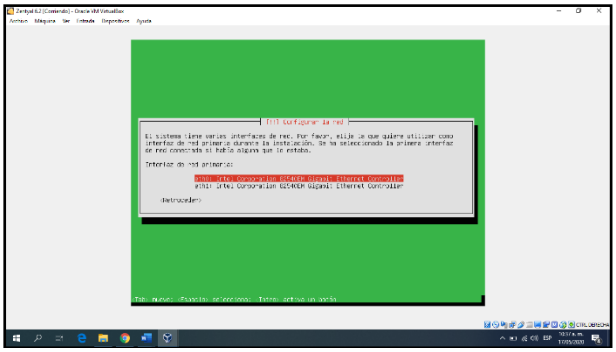

Figura 4 Selección de interfaz de red

Se procedió con la configuración de los datos de nombre de la máquina.

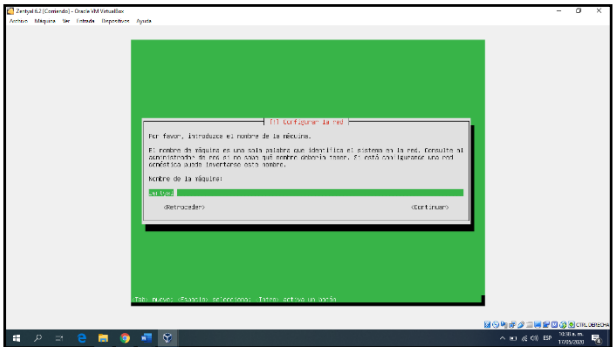

Figura 5 Configuración de cuentas

Se realizó la configuración de la cuenta de usuario, contraseña y se confirmó la configuración de la zona horaria para que el sistema comenzara la instalación.

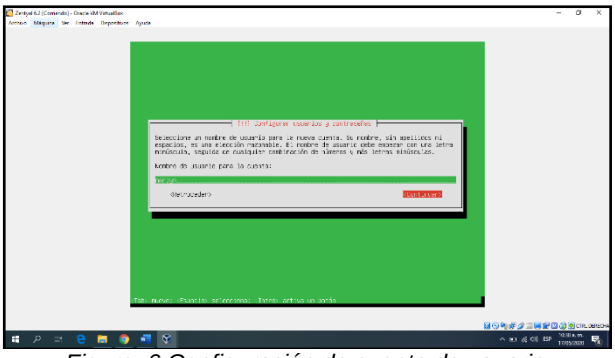

Figura 6 Configuración de cuenta de usuario

Una vez finalizó el proceso de instalación del sistema, se ingresó al panel de control con el usuario y contraseña definidos y se comenzó a usar los servicios.

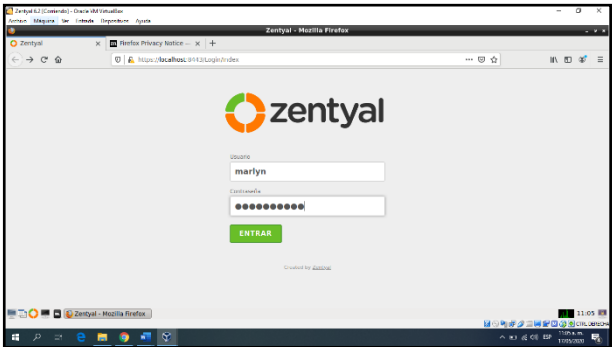

Figura 7 Inicio de sesión

3 CONFIGURACIÓN DE ZENTYAL

3.1 DHCP SERVER, DNS SERVER Y CONTROLADOR DE DOMINIO.

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 Debian 10 a través de un usuario y contraseña, así como también el registro de dicha estación en los servicios de Infraestructura IT de Zentyal.

Se procedió a escoger los servicios, los cuales fueron:

- Directorio activo
- DHCP
- DNS.

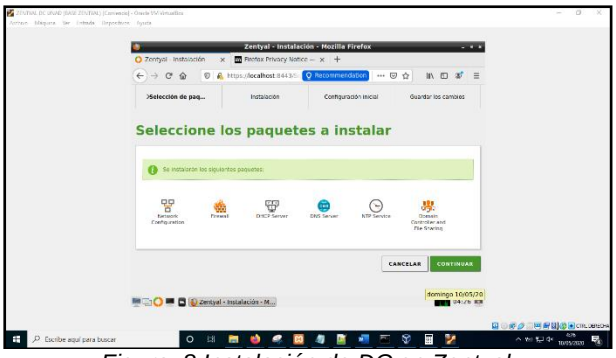

Figura 8 Instalación de DC en Zentyal

La IP asignada a nuestro servidor Zentyal se estableció como 192.168.1.225. Se usó el nombre por defecto que nos sugiere el sistema “zentyal-domain.lan”.

Se procedió a configurar le servicio de DHCP. El rango inició 192.168.1.227 y terminó en 192.168.1.233.

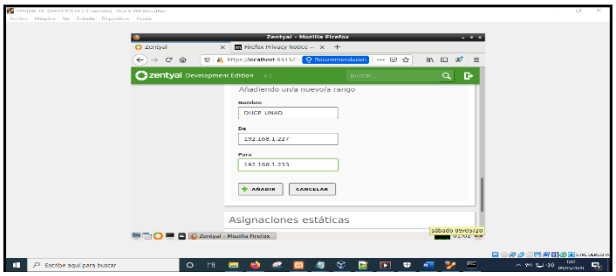

Figura 9 Configuración DHCP

Nombre DNS “zentyal-domain-lan” con ello se buscó que los equipos que se configuraron para pertenecer o hacer parte del DC pudieran encontrar y enrutar gracias al DHCP y DNS, las rutas correctas para comunicarse con el Zentyal y su DC.

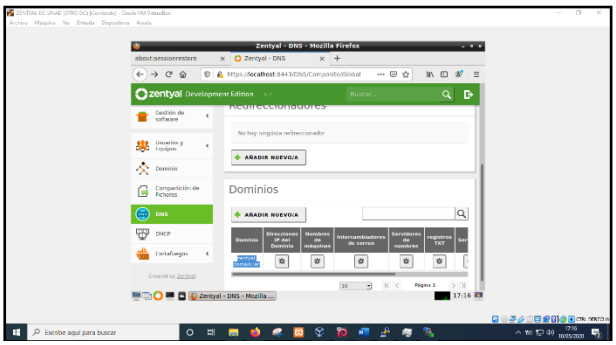

Figura 10 Configuración DNS

Se procedió a instalar módulo “msjtutil” el cual ayudó a realizar la conexión al DC por medio de Kerberos. Con el comando “sudo apt-get install sssd heimdal-clients msktutil” se realizó la instalación.

Se procedió a modificar la configuración mediante el comando “sudo /etc/krb5.conf” con el respectivo código, donde la función “default_realm” definió la conexión a nuestro DC Zentyal.

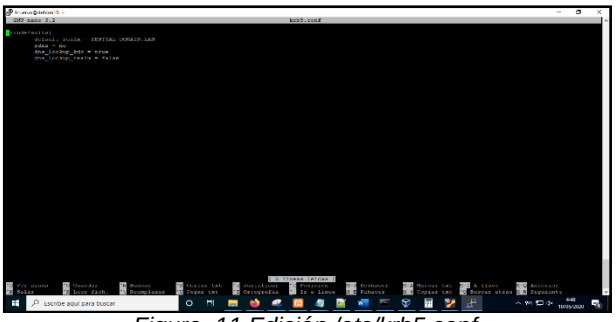

Figura 11 Edición /etc/krb5.conf

Se editó la ruta “/etc/hosts/” en el archivo y se agregó la línea “127.0.1.1 lubuntu.zentyal-domain.lan Lubuntu” [2]

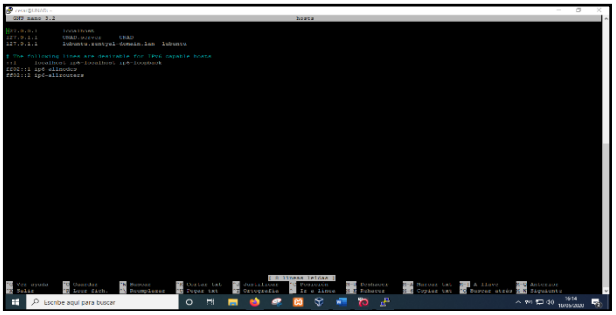

Figura 12 Edición del archivo /etc/hosts

Luego, con el comando “sudo kinit Administrator” se procedió a iniciar sesión por medio del puerto TCP 88 del servicio de Kerberos en nuestro Zentyal. Se ingresó la contraseña del usuario Administrador. Luego de realizar la conexión, se comprobó por medio del comando “klist”, que la conexión fue satisfactoria. Lo que indicó que se había establecido conexión al DC desde Linux Debian por medio de Kerberos.

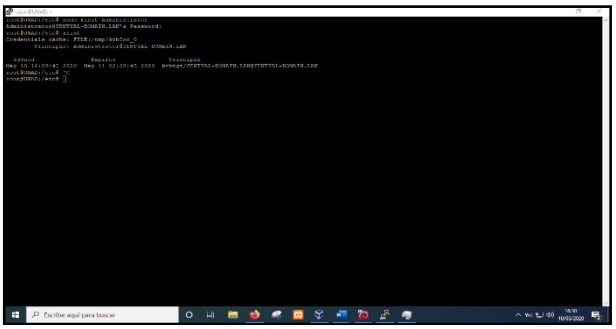

Figura 13 Conexión con kinit a kerberos

Luego se procedió a agregar el equipo Debian al DC, para esto fue necesario asignarle un nombre netbios, en este caso el nombre usado fue “Lubuntu”. Por medio de los siguientes comandos se realizó la operación: “sudo msktutil -N -c -b 'CN=COMPUTERS' -s HOST/lubuntu.zentyal-domain.lan -k test.keytab --computer-name LUBUNTU --upn LUBUNTU$ --server zentyal.zentyal-domain.lan --user-creds-only –verbose [2]

Luego se usó el comando sudo msktutil -N -c -b 'CN=COMPUTERS' -s HOST/lubuntu -k test.keytab --

computer-name LUBUNTU --upn LUBUNTU$ --server zentyal.zentyal-domain.lan --user-creds-only –verbose" [2]

A continuación, se observó nuestro Zentyal y pudimos ver que el equipo Debian estaba bajo nombre netbios "Lubuntu" dentro del DC.

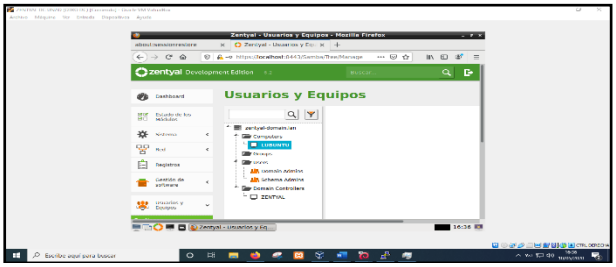

Figura 14 UA del DC con equipo Debian 10 agregado

Luego se procedió con la desconexión del servicio de Kerberos mediante el comando "kdestroy". Con esto se cancelaron las credenciales que tenía en el momento. Se debió configurar nuestro inicio de sesión en Debian para que pudiera conectarse al servidor DC. Se procedió a realizar edición del archivo que se encuentra en la ruta "/etc/sssd/sssd.conf"

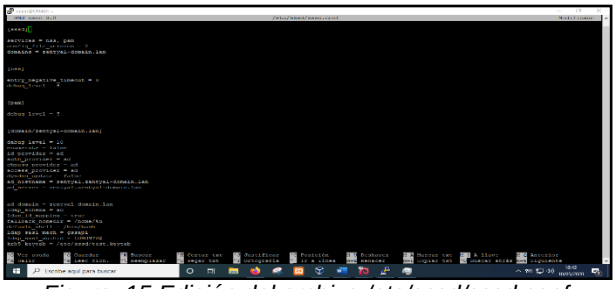

Figura 15 Edición del archivo /etc/sssd/sssd.conf

Con lo anterior se buscó que el "SSSD" o "System Security Services Daemon" nos ayudara a iniciar sesión dentro de nuestro DC "zentyal-domain.lan". Cuando terminamos de editar el archivo en la ruta "/etc/sssd" se procedió a ejecutar el comando "sudo chmod 0600 sssd.conf" con el fin de darle permiso de "0600" [2]

Se reinició el servicio "SSSD" y se comprobó que no genera error alguno.

Luego se procedió a editar en la ruta "/etc/pam.d/common-session" buscando la línea "session required pam_unix.so" y agregamos bajo esta la línea "session required pam_mkhomedir.so skel=/etc/skel umask=0077" [2]

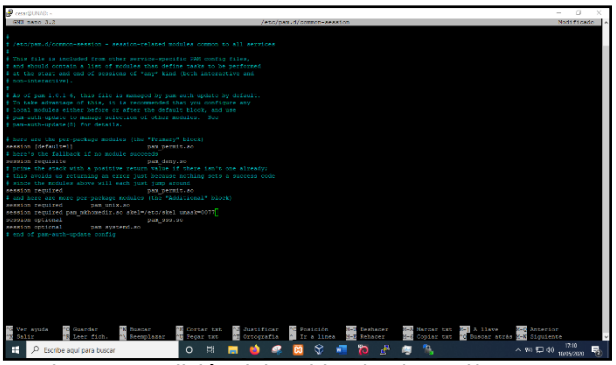

Figura 16 Edición del archivo /etc/pam.d/common-session

Se procedió a crear el usuario "pruebas" en nuestro DC Zentyal, con el fin de que este iniciara sesión desde nuestro Debían.

Se inició sesión con el usuario "pruebas" de nuestro DC.

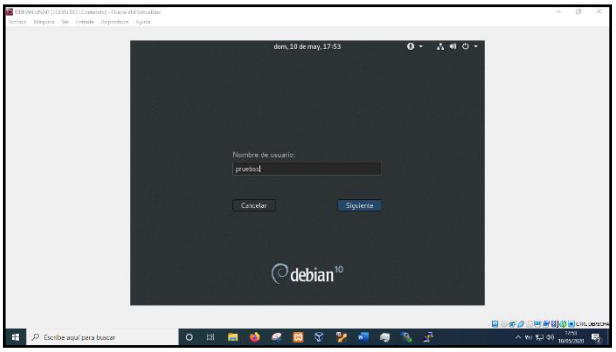

Figura 17 Inicio sesión Debian 10 en DC Zentyal

Se observó el inicio de sesión satisfactorio en nuestro Linux Debian 10.

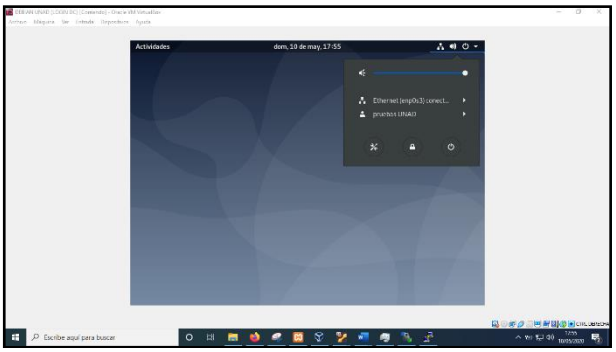

Figura 18 Escritorio Debian 10 bajo usuario autenticado en DC Zentyal

3.2 PROXY NO TRANSPARENTE

Temática 2: Proxy no transparente

Producto esperado: Implementación y configuración detallada del control del acceso de una estación GNU/Linux Debian 10 a los servicios de

conectividad a Internet desde Zentyal a través de un proxy que filtra la salida por medio del puerto 830.

Fue importante considerar los adaptadores de red que se usaron para el desarrollo de la actividad tanto para el servidor Zentyal 6.2, como para la estación Debian 10.

Zentyal 6.2: el Adaptador 1 (eth2) como adaptador puente y el Adaptador 2 (eth1) como red interna (con la que se conectó Debian 10) con nombre ZENTYAL-LAN.

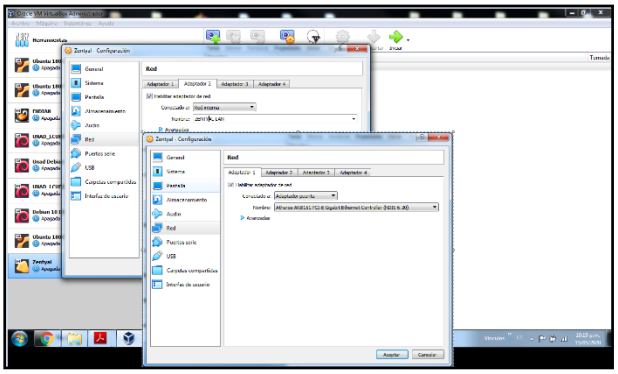

Figura 19 Pantalla configuración Máquina VirtuaBox para Zentyal 6.2.

Debian 10: el Adaptador 1 como red interna, Asociada a ZENTYAL-LAN, del paso anterior.

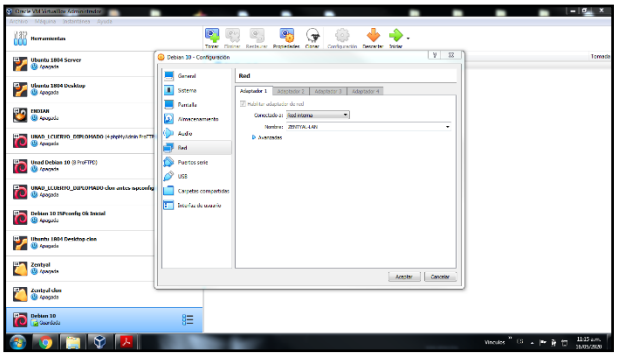

Figura 20 Pantalla configuración Máquina VirtuaBox Para Debian 10.

En el proceso de instalación de Zentyal 6.2 fue necesario activar DC (Domain Controller), DNS (Sistema de nombres de dominio), DHCP (Dynamic Host Configuration Protocol), Firewall y HTTP Proxy.

En Red/Objetos, se creó objeto ClienteDebian y se ingresó miembro con nombre “lcuervoc” y la respectiva IP asociada asignada por DHCP de red interna en este caso fue “192.168.15.100”

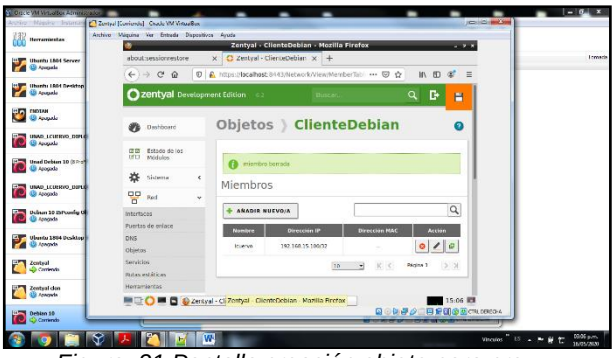

Figura 21 Pantalla creación objeto para proxy.

En Proxy HTTP en Reglas de acceso, se configuró como origen objeto de Red “ClienteDebian”, nótese que no se marcó la opción Proxy Transparente, por lo tanto, la configuración se adecuaba al Proxy No Transparente y también se asignó el puerto que requería la actividad, 830 en este caso.

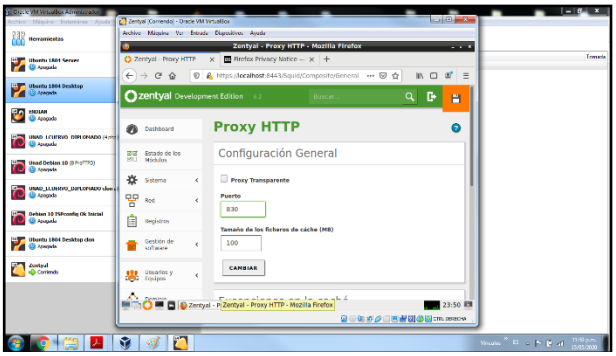

Figura 22 Pantalla configuración puerto proxy.

Se configuró la dirección IP a la 192.168.15.1 en la interfaz de red eth1.

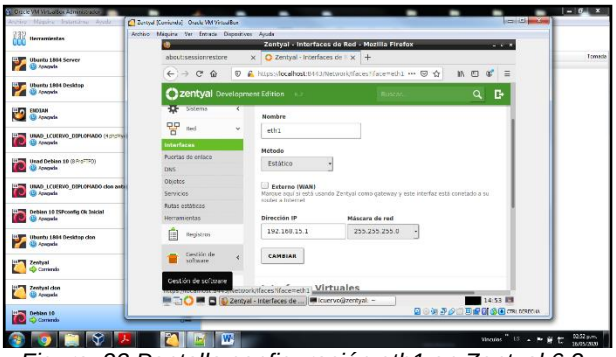

Figura 23 Pantalla configuración eth1 en Zentyal 6.2.

Después en DHCP configuraciones se creó un rango con nombre DHCP_DIPL y RANGO 192.168.15.100 a 192.168.15.115 para asignación DHCP de la red interna de Zentyal 6.2.

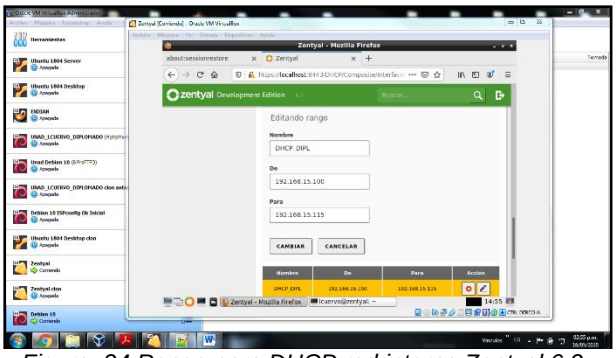

Figura 24 Rango para DHCP red interna Zentyal 6.2.

Al reiniciar Debian 10, Zentyal asignó la IP 192.168.15.100 cómo se visualiza en la siguiente imagen.

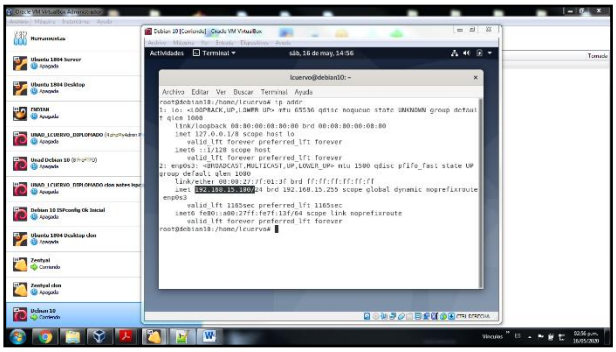

Figura 25 Pantalla IP asignada en Debian 10 por DHCP Zentyal 6.2.

Por otro lado, Zentyal 6.2 identificó la estación Debian 10 correctamente.

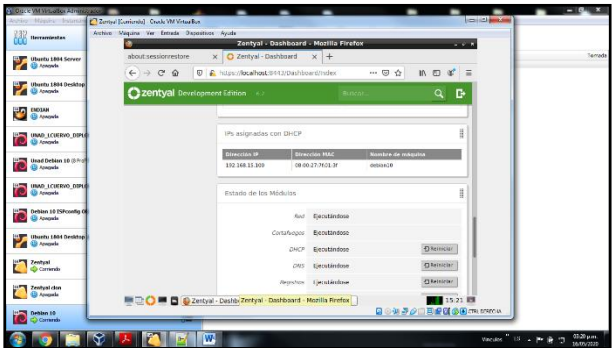

Figura 26 Pantalla IP asignada a Debian 10 por DHCP Zentyal 6.2

Inicialmente tuvimos acceso full a páginas web desde la estación Debian 10, debido a que las reglas de acceso del proxy estaban abiertas desde cualquier origen.

Se procedió a configurar las reglas de nuestro proxy para que restringiera todo el tráfico a internet desde la estación Debian 10.

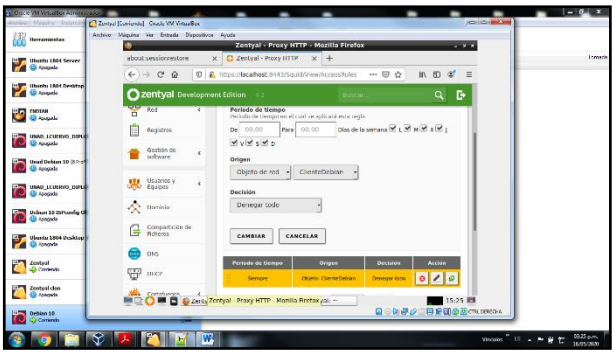

Figura 27 Pantalla denegación tráfico por Proxy.

Ahora se configuró el proxy en la estación Debian 10, opción Proxy de la red y se cambió el acceso a 192.168.15.1 por puerto 830

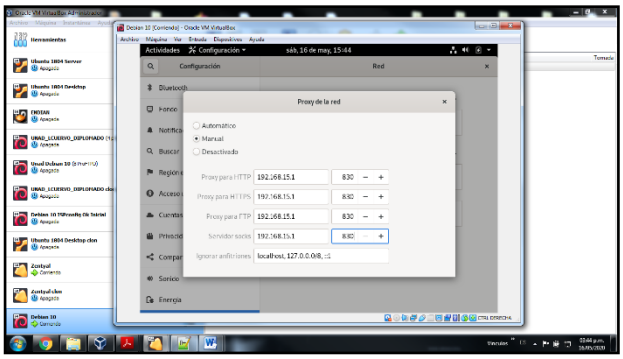

Figura 28 Pantalla configuración acceso por proxy desde estación Debian 10.

La configuración por medio de perfil de filtrado permitió un mayor control por red que la asociada a un objeto de red.

En Debian 10, se confirmó acceso a internet, y efectivamente estaba restringiendo todos los accesos, tal cual como lo configuramos en Zentyal 6.2.

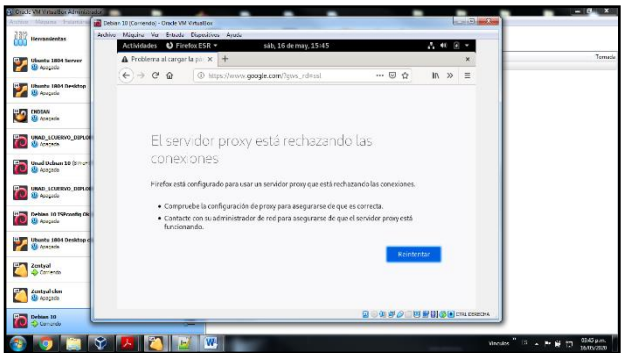

Figura 29 Pantalla de restricción de acceso a internet en estación Debian 10.

3.3 CORTAFUEGOS

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 Debian 10.

Se seleccionaron los paquetes de Zentyal a instalar los cuales fueron DNS Server, DHCP Server y Firewall.

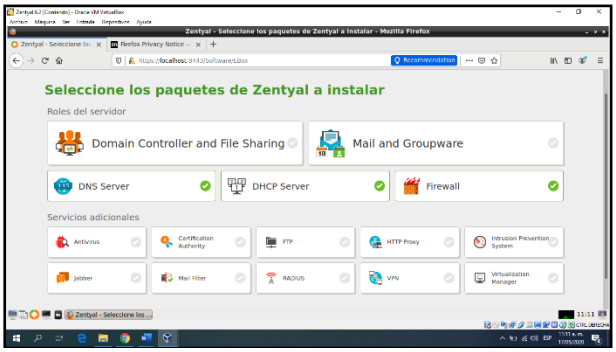

Figura 30 Paquetes de Zentyal a instalar

Se configuraron las interfaces de red de la siguiente manera: eth0 como red externa (WAN) y eht1 como red interna (LAN).

Figura 31 Configuración de interfaces de red

Se configuraron las redes para las interfaces externas de la siguiente manera: eth0 por DHCP y eth1 como estática asignando la IP: 192.168.0.254

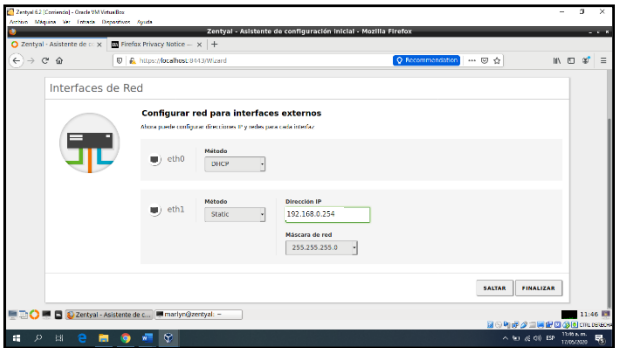

Figura 32 Configuración de redes para las interfaces

Se configuraron los servicios DHCP por medio de Zentyal asignando un rango dentro del segmento de red, para que la máquina cliente tomara una IP del rango asignado.

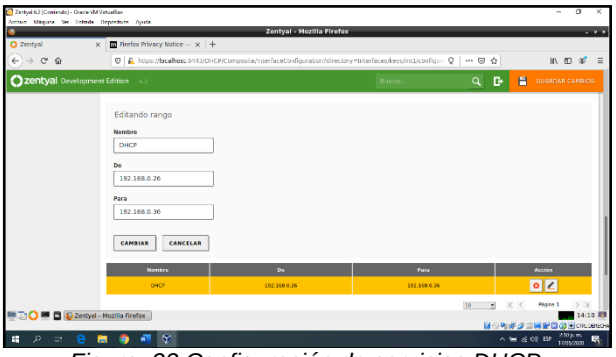

Figura 33 Configuración de servicios DHCP

En la máquina cliente, se configuró el adaptador 1 como red interna y se seleccionó la red creada por medio de Zentyal como Zentyal_LAN. Se observó que la máquina cliente tomó una dirección IP del rango asignado.

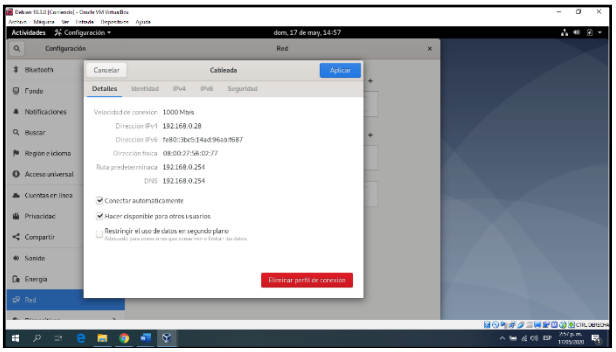

Figura 34 Configuración de red en Máquina cliente

Se verificó el acceso a desde la máquina cliente a los sitios de entretenimiento y redes sociales identificando que se tenía acceso correctamente.

Figura 35 Verificación de acceso a sitios

Se utilizó el comando nslookup para obtener la dirección IP de cada uno de los sitios en los cuales se iba a restringir el acceso. Existió un caso especial para YouTube, para soportar una red grande y creciente de servidores web, YouTube tiene varias direcciones IP.

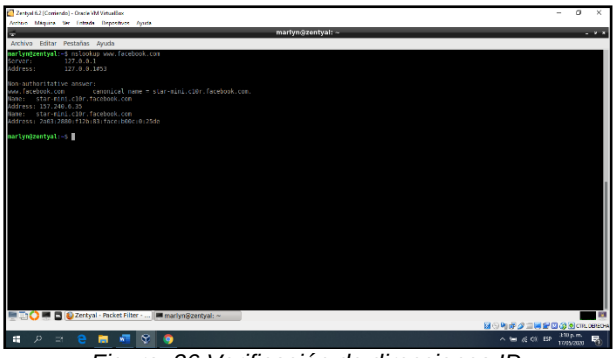

Figura 36 Verificación de direcciones IP

Fue necesario acceder a la opción reglas de filtrado para las redes internas para configurarlas.

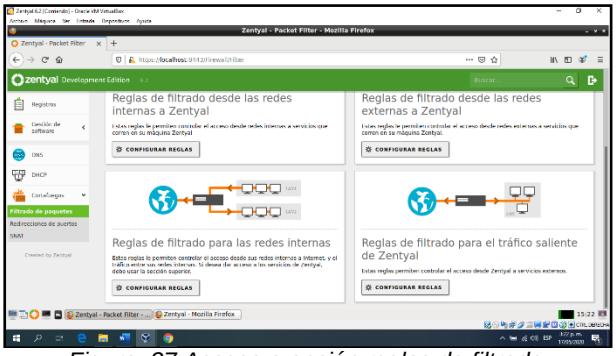

Figura 37 Acceso a opción reglas de filtrado

Se crearon las reglas de bloqueo de los sitios de entretenimiento y redes sociales, denegando los permisos desde cualquier origen hasta la dirección IP del sitio.

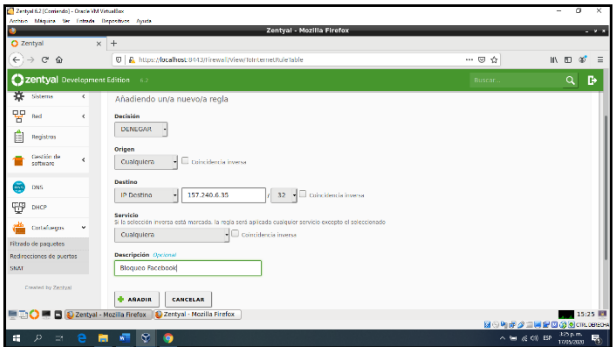

Figura 38 Creación de regla de acceso

Una vez se asignaron todas las reglas, estas se evidenciaron en el panel de filtrado de paquetes. Para que se tomaran los cambios y estos pudieran ser replicados en la red, se aplicó la opción guardar.

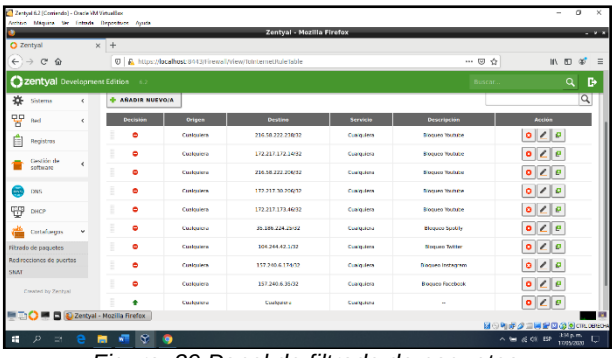

Figura 39 Panel de filtrado de paquetes

Se verificó el acceso a internet desde la máquina cliente y se evidenció que se pudo acceder de manera correcta.

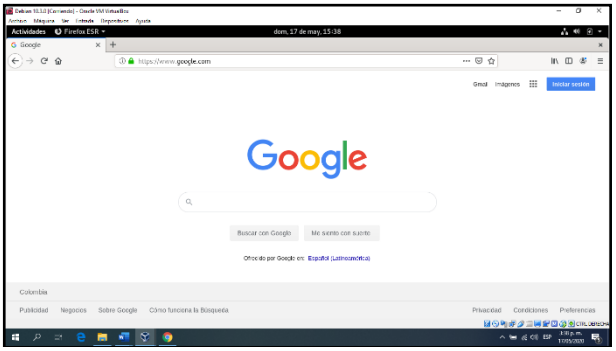

Figura 40 Verificación de acceso a internet

Se verificó el acceso a cada uno de los sitios bloqueados por medio de la regla evidenciándose que fueron aplicadas y no se permitió el acceso a los sitios.

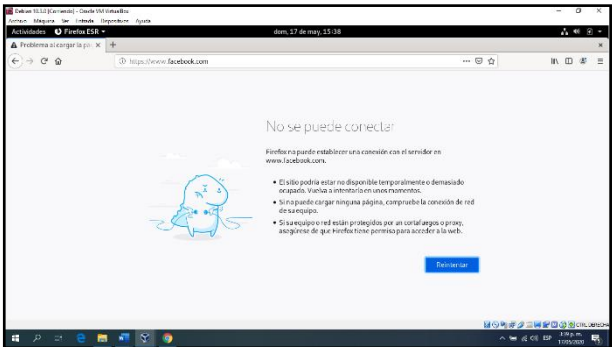

Figura 41 Verificación de aplicación de la regla

3.4 FILE SERVER Y PRINT SERVER

Temática 4: File Server y Print Server
Producto esperado: Implementación y configuración detallada del acceso de una estación de trabajo GNU/Linux Debian 10 a través del controlador de dominio LDAP a los servicios de carpetas compartidas e impresoras

Zentyal usa el protocolo SMB/CIFS para mantener la compatibilidad con los clientes Microsoft. Una vez se

configuró correctamente el controlador de dominio, el servidor permitió activar los servicios de servidor de ficheros SMB/CIFS, para lo cual se usó LDAP, como servicio de directorio, con tecnología Samba para implementar la funcionalidad de controlador de dominios Windows, además para la compartición de ficheros e impresoras [4]. LADP se configuró por defecto con la configuración del DNS. Posteriormente fue posible administrar en el apartado grupos y usuarios, quiénes podrían hacer uso de los recursos compartidos e incluso para acceso a través del dominio y de las directivas de control que la entidad estipule [4].

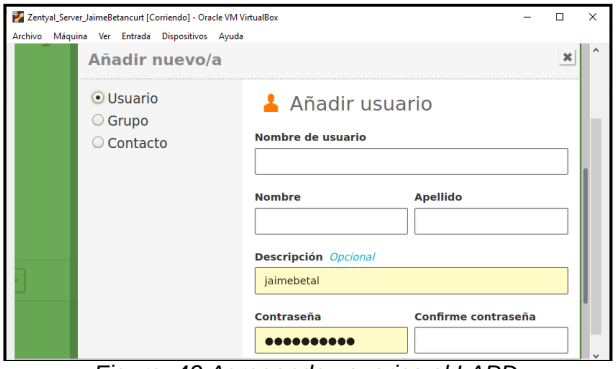

Figura 42 Agregando usuarios al LAPD

En este apartado sólo debió asignarse el nombre del recurso a crear y la ruta en la cual se crearía, que por defecto utilizó el directorio bajo Zentyal en la ruta /home/samba/shares.

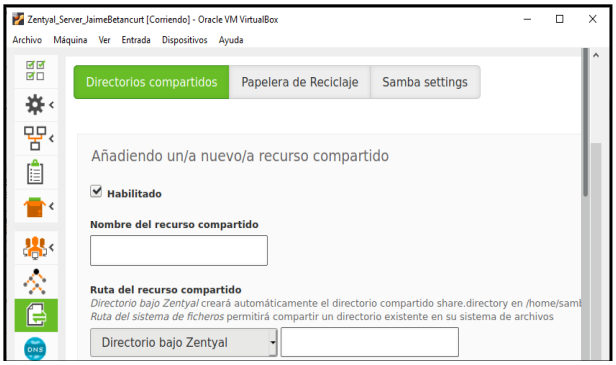

Figura 43 Creando un recurso compartido

Una vez se almacenaron los cambios, se desplegó el listado de recursos creados, con las opciones de configuración ACL. Fue posible incluso editar los usuarios que podían acceder y los permisos que se asignarían sobre la carpeta [4].

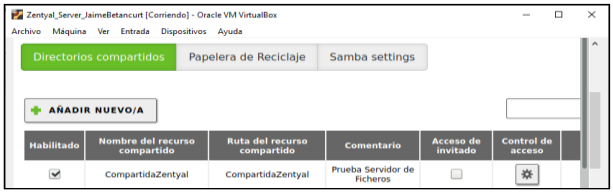

Figura 44 Listado de recursos compartidos

Fue posible acceder a los recursos compartidos realizando configuraciones adecuadas en cada equipo cliente. Fue necesario que el cliente se reconociera por el controlador de dominio, por lo cual debimos tener en cuenta lo realizado en el numeral 3 temática 1 de este documento, donde se conectó un equipo Linux al Directorio Activo de Zentyal.

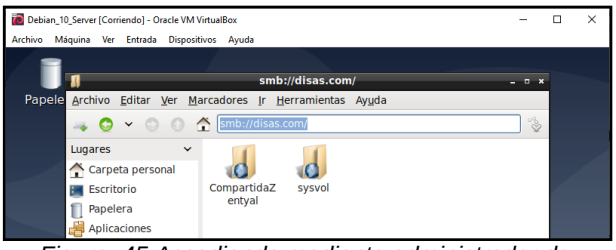

Figura 45 Accediendo mediante administrador de archivos

Hecho lo anterior y a través del gestor de archivos, se accedió a la barra de direcciones y se escribió el comando smb://<equiporemoto>. En este caso se usó el nombre del dominio local *smb://disas.com*. Lo anterior cargó los recursos compartidos en el servidor. Se accedió a uno de los recursos compartidos para terminar de configurarlo, cargando un formulario en el cual debía diligenciarse los datos del usuario al cual se le otorgaron permisos en Zentyal. Para tener acceso permanente al recurso se marcó la opción recordar para siempre.

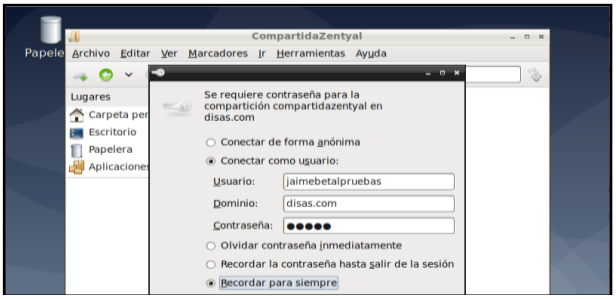

Figura 46 Configuración del recurso compartido

Finalmente se montó el recurso como un lugar accesible desde el administrador de archivos.

Figura 47 Accediendo al recurso compartido desde Debian

Para el servidor de impresoras, se utilizó el software CUPS. Este viene acompañado de una interfaz web en la cual se gestionan las impresoras del servidor. En Zentyal 6.2 no viene integrado en su instalación, por lo cual se realizó de forma manual. Esto no garantizó el acceso remoto al servicio, pues Zentyal agregó las reglas de navegación del firewall al instalar los módulos y en este

caso debió hacerse de forma manual, agregando una regla TCP para este servicio.

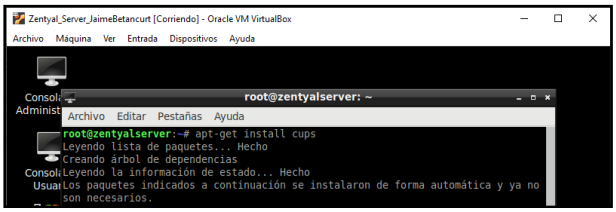

Figura 48 Instalación de CUPS en Zentyal

CUPS se administró a través de su propia interfaz web a la cual se accedió de manera local con la dirección https://<equipolocal>:631. Al ingresar se solicitaron credenciales del usuario actual. Se requería ser *root* para instalar la impresora. Una vez logueados cargó el panel de administración web.

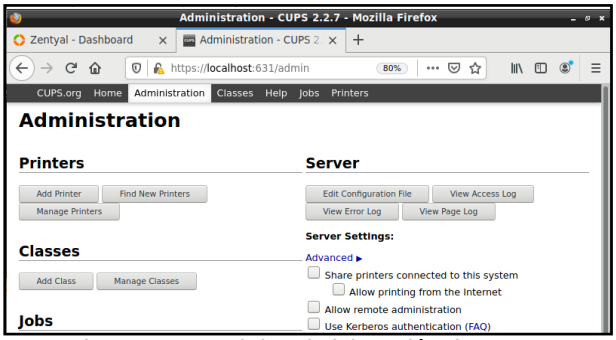

Figura 49 Panel de administración de CUPS

Para que las impresoras instaladas pudieran ser accedidas a través de la red, debió desplegarse el menú Server Settings y activar la opción compartir impresoras conectadas a este sistema. Además, para poder administrar desde otro quipo la aplicación CUPS, se activó la opción Permitir administración remota [4].

Se conectó una impresora HP Inktank 310 al equipo anfitrión y se configuró el apartado USB de la máquina virtual Zentyal, para que reconociera la impresora. Al iniciar el panel de administración web de CUPS, se inició con la opción Agregar impresora y esta fue efectivamente reconocida. La instalación continuó con un formulario donde se diligenciaron datos como nombre a asignar al recurso, ubicación y descripción. Es importante marcar la opción Compartir esta impresora.

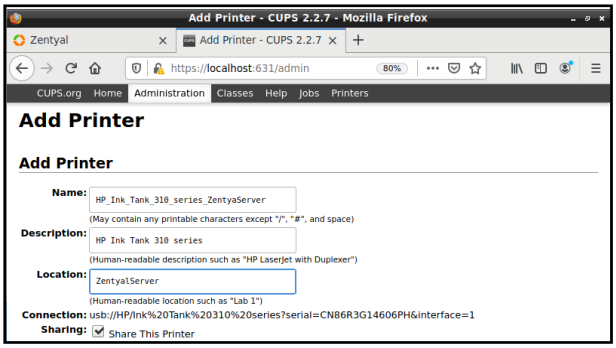

Figura 50 Formulario agregar impresora

Una vez se continuó con el proceso el asistente solicitó seleccionar el modelo de la impresora a instalar. Finalmente se mostraron las opciones de configuración de impresión predeterminadas, en las cuales dejamos las opciones por defecto. De esta manera se ha instaló adecuadamente una impresora para luego tener acceso desde la red [6].

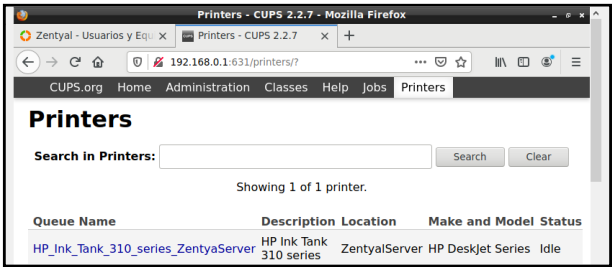

Figura 51 Listado de impresoras en el servidor

En Debían se procedió también con la ejecución de CUPS de manera local el cual venía ya instalado. Accedimos al panel de administración web y repetimos los mismos pasos de la instalación en el servidor. Primero se obtuvo la dirección de red en el panel de administración de Zentyal, menú administrar impresoras, para lo cual en la impresora que íbamos a instalar hicimos clic derecho sobre el nombre y seleccionamos la opción copiar la ruta de enlace [6]. Esta fue la dirección que en Debian debimos escribir en la opción Conexión, del panel de administración.

Figura 52 Listado de impresoras en Debian

3.5 VPN

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 Debian 10. Se debe evidenciar el ingreso a algún contenido o aplicación de la estación de trabajo.

Primero fue necesario crear un VPN servidor.

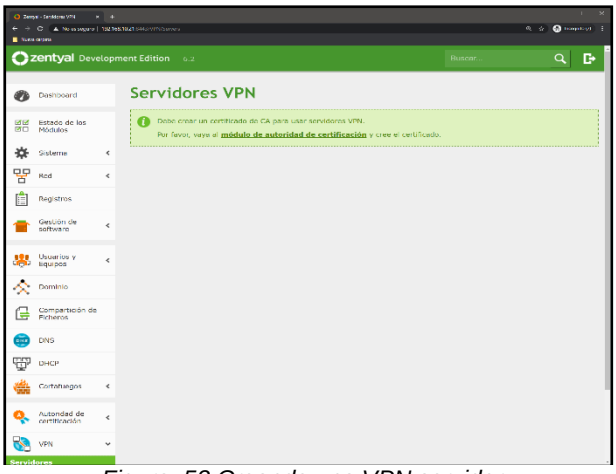

Figura 53 Creando una VPN servidor.

Para que la VPN funcionara se debían crear autoridades certificadoras, que asignan el permiso de entrada a la VPN.

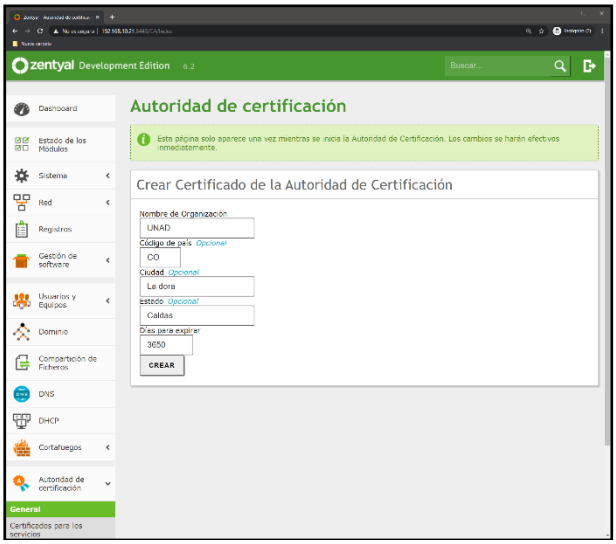

Figura 54 Autoridades certificadoras

Se añadió, luego de la creación de las autoridades, un nuevo servidor al cual se le asignó un nombre y se habilitó. En este servidor es donde se guardaron las configuraciones, para luego proceder a verificar la configuración Server VPN y habilitar la interfaz TUN.

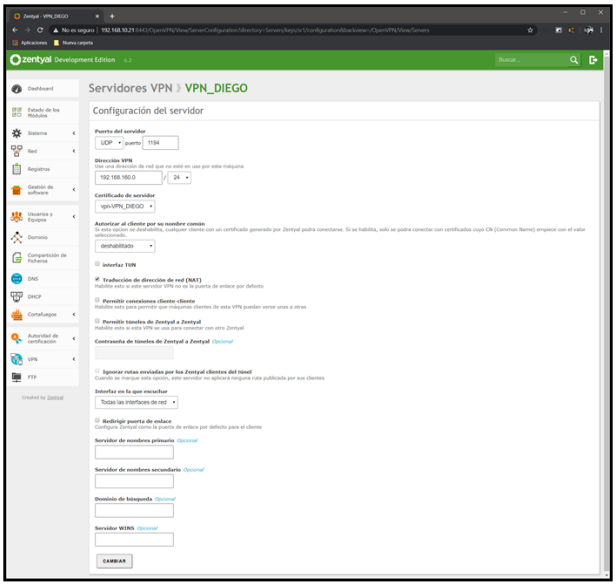

Figura 55 Red 192.168.20.0/24

En las listas de redes anunciadas se mostraron las redes que eran visibles desde la VPN. En este ejemplo se accedió al servidor Debian configurándolo con una IP 192.168.20.2 por lo cual se agregó la red 192.168.20.0/24 y se añadió un certificado VPN.

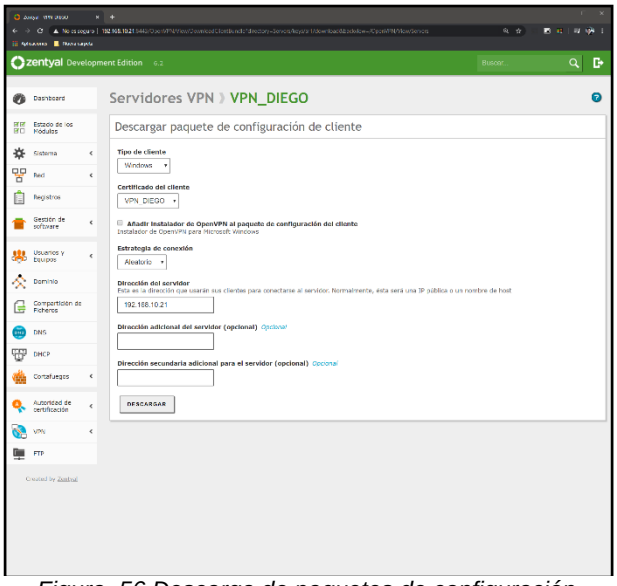

Figura 56 Descarga de paquetes de configuración

Se descargó el paquete de configuración del cliente.

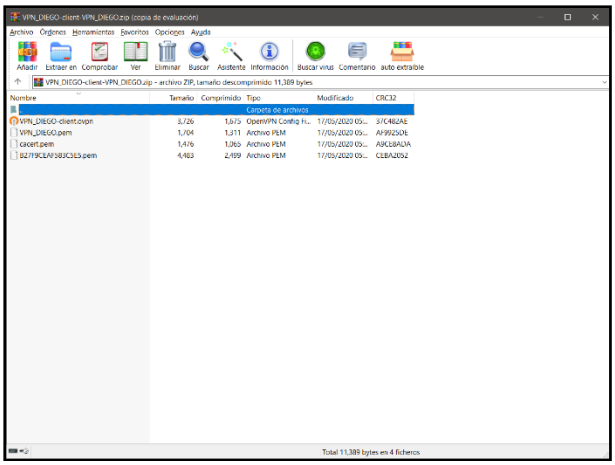

Figura 57 Paquete de configuración del cliente

Se instaló cliente VPN en nuestro cliente remoto.

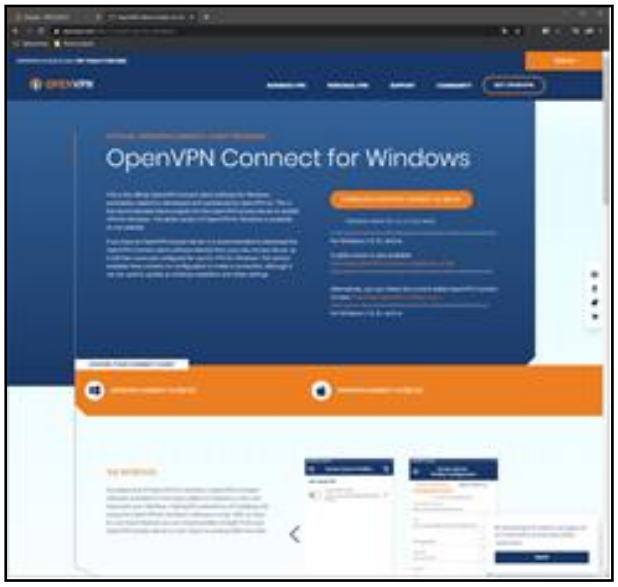

Figura 58 VPN en nuestro cliente remoto

Después de todos los pasos fue necesario hacer la verificación, comprobando que no teníamos acceso a la IP remota del servidor.

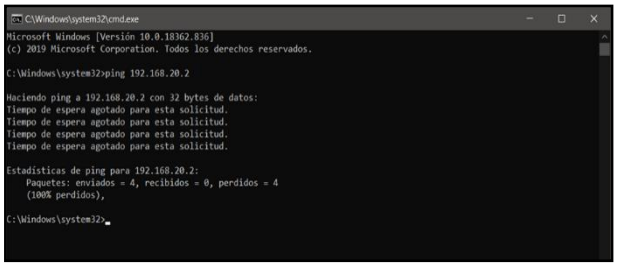

Figura 59 Verificación del acceso a la IP remota del servidor.

Se configuró VPNCONNECT.

Figura 60 Openvpn Connect

Se comprobó el acceso al Server de la red remota.

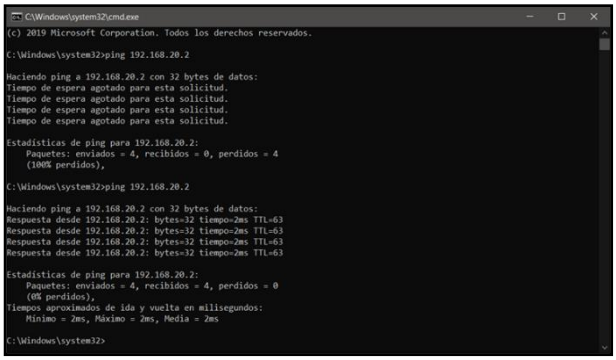

Figura 61 Verificación del acceso al Server

Una vez se comprobó la conexión y el servidor VPN, fue posible verificar el acceso a través de un ping y verificar que los servicios como web podían ser accedidos desde el cliente remoto.

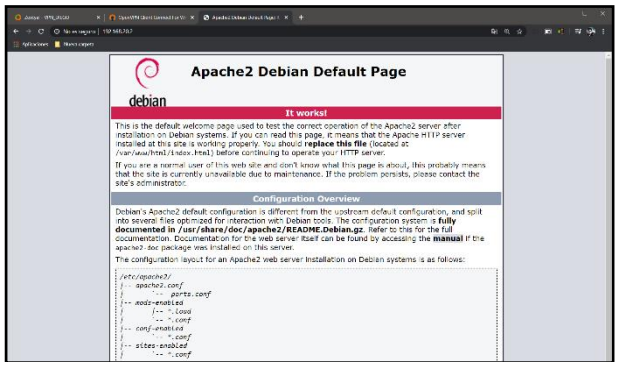

Figura 62 Verificación en Debian

4 CONCLUSIONES

Zentyal incluye los paquetes de instalación de servicios propios del servidor, lo que no sucede con otras distribuciones probadas y que en definitiva ahorra mucho trabajo. La administración del servidor es algo intuitiva y la curva de aprendizaje es moderadamente rápida. Otro aspecto a favor es el panel de administración que presenta un diseño muy elaborado, de fácil reconocimiento el cual es una poderosa herramienta que Zentyal ofrece y desde donde es posible configurar cada uno de los módulos que se activen en el servidor.

Zentyal como DC es una herramienta fuerte para entornos no mayores de 20 estaciones de trabajo, las configuraciones básicas de autenticación y centralización de políticas ayudan en la administración eficiente de nuestros activos informáticos. La aplicación de inicio de sesión a equipos Linux es una herramienta eficaz de control de usuarios, donde podemos unificar tanto sistemas Linux como Windows en un DC en inicio de sesión seguro y controlado. Los servicios de DC son recomendados como buena práctica tenerlos de manera independiente, debido que si estos dependen de otros servicios como BD o Servidor Web pueden afectar el funcionamiento del DC al reiniciar o actualizar este tipo de servicios.

Es primordial supervisar los accesos a páginas web de internet, con el fin de controlar salida y entrada de información, pudiendo así evitar posibles daños o perjuicios en nuestra plataforma; el proxy es una herramienta indispensable para tal fin, y combinado con otras herramientas hace que sea más segura la red.

Desde la concepción de un sistema de información se deben tener en cuenta todos los parámetros de seguridad con el fin de entregar un producto confiable al usuario final o si es el caso, para tener una garantía de nuestra propia seguridad y esto hace parte del aseguramiento de la calidad del sistema. Los diferentes firewalls o cortafuegos proporcionan protección en cuanto a los accesos a las redes informáticas, es por esto, por lo que es importante tener un amplio conocimiento sobre la instalación y correcta configuración de estos sistemas de seguridad con el fin de implementar reglas que nos ayuden a regular el tráfico de nuestras redes y las formas de conectarnos, todo esto con el propósito de hacer más seguros nuestros sistemas de información.

Zentyal configura por defecto aspectos básicos en servicios como el Cortafuegos o el DNS permitiendo el acceso a los servicios instalados, agregando las excepciones de acceso remoto al servidor, por cada uno de los módulos configurados. El proceso que permite convertir a Zentyal en un servidor de archivos es muy sencillo y gracias a sus módulos integrados, el acceso remoto no requiere de configuraciones extremas. Si embargo aun cuando existen una serie de herramientas que permiten conectar máquinas Linux al Directorio Activo LAPD y al Controlador de Dominio, la mayoría requieren de complejos pasos que implican instalación de aplicaciones a través de la consola, además de la posterior modificación de archivos de configuración.

Aunque actualmente se usa Kerberos instalando la herramienta *heimdal-clients*, para junto con SAMBA realizar la conexión del cliente al dominio creado en Zentyal se pudo probar otra herramienta poco menos complicada y extensa de configurar llamada Power Broker Identity Services o *pbis-open*, que luego de una instalación manual, ya que no se soporta en repositorios, permite conectar fácilmente el equipo al dominio.

El servidor de impresoras CUPS no viene integrado, al menos en la versión 6.2 usada en este paso, por lo cual fue necesario instalarlo de forma manual y acceder al panel Web de este servicio de forma externa al panel de Zentyal, lo cual no garantiza que se pueda acceder de forma remota a CUPS, pues es necesario crear una regla de navegación en el cortafuegos, que permita acceder al panel de administración CUPS en Zentyal, desde otro equipo en la red.

Es importante resaltar que se puede configurar Zentyal para dar soporte a clientes remotos (conocidos como Road Warriors). Esto es, un servidor Zentyal trabajando como puerta de enlace y como servidor VPN, que tiene varias redes de área local (LAN) detrás, permitiendo a clientes externos (los road warriors) conectarse a dichas redes locales vía servicio VPN.

5 REFERENCIAS

[1] López Manjarrez, J. F. “Configuración e implementación del Zentyal server 6.0 como una Virtual Private Network (VPN)”. (2019). [En línea]. Disponible en: https://repository.unad.edu.co/handle/10596/31954

[2] Zentyal. “Authenticating Linux client against Samba”. (2014). [En línea]. Disponible en: https://wiki.zentyal.org/wiki/Authenticating_Linux_client_against_Samba

[3] Zentyal, *“Configuración de un cortafuegos con Zentyal”.* (2018) [En línea]. Disponible en: https://doc.zentyal.org/es/firewall.html

[4] Zentyal, “*Configurar un servidor de ficheros con Zentyal*”, (2015). [En línea]. Disponible en: https://wiki.zentyal.org

[5] Zentyal, “*Facilita la gestión de tu infraestructura TIC*”, (2020). [En línea]. Disponible en: https://zentyal.com/es/caracteristicas/

[6] Zentyal, “*Servicio de compartición de impresoras”*, (2015). [En línea]. Disponible en: https://wiki.zentyal.org

[7] Zentyal, “*Servicio de configuración de red (DHCP)*”, (2014). [En línea]. Disponible en: https://wiki.zentyal.org

[8] Zentyal *“Servicio de Proxy HTTP”* (2018). Disponible en: https://doc.zentyal.org/es/proxy.html