DIPLOMADO DE PROFUNDIZACIÓN EN LINUX (OPCIÓN DE TRABAJO DE GRADO) 201494A_614 EVALUACIÓN FINAL PASO 8

Sirladys Yisela Carrillo
e-mail: sisycarrillo@gmail.com
Mayte Dayana Cerón
e-mail: maitedayana26@hotmail.com
Deybison Smith Martinez Lidueñas
e-mail: deybisonmartinez@hotmail.com
Mario Luis Guzman
e-mail: meva_82@hotmail.com
Camilo Andres Vega.
e-mail: cavegag@unadvirtual.edu.co

RESUMEN: *El presente documento muestra el proceso realizado para instalación y configuración del servidor Zentyal 5.0 como sistema operativo, sobre el cual se implementan los servicios y plataformas DHCP Server, DNS Server y Controlador de Dominio, Proxy no transparente, Cortafuegos y VPN.*

ABSTRACT: *This document shows the process carried out for installation and configuration of the Zentyal 5.0 server as an operating system, on which the DHCP Server, DNS Server and Domain Controller, Nontransparent Proxy, Firewall and VPN services and platforms are implemented.*

PALABRAS CLAVE:
.
- Controlador de Dominio
- Cortafuegos
- File Server
- Proxy
- VPN

1 Introducción

El presente documento tiene como objetivo el desarrollo de la actividad Paso 8 – Solucionando necesidades específicas con GNU/Linux, Trabajo del curso Diplomado de profundización en Linux (Opción de grado) de la universidad nacional abierta y a distancia UNAD.

En el trabajo se realizan ejercicio de instalación y configuración de Zentyal, herramienta por el cual ayuda la administración de infraestructura de una compañía. Todo esto ayuda a obtener habilidades de planear la gestión de seguridad y la estructuración de permisos con el fin de administrar y compartir específicamente los recursos del sistema atendiendo las necesidades de los usuarios.

Con las actividades realizadas en este documento podremos aumentar nuestros conocimientos en Linux.

2 Instalación de Zentyal Server 5.0

2.1 Requisitos

El servidor Zentyal puede funcionar sin ningún problema con 2 Gb de RAM, 10 GB de Disco Duro y un procesador de doble núcleo. Además es importante tener en cuenta la instalación de dos tarjetas de red para la configuración de la red externa WAN y la red Interna LAN.

2.2 URL de descarga

Se descarga Zentyal Server 5.0 desde http://download.zentyal.com/zentyal-5.0.1-development-amd64.iso. Este será el archivo .iso que contiene la imagen para la instalación de Zentyal Server.

2.3 Proceso de Instalación

En una máquina virtual de VirtualBox, se comienza la instalación booteando desde la imagen descargada:

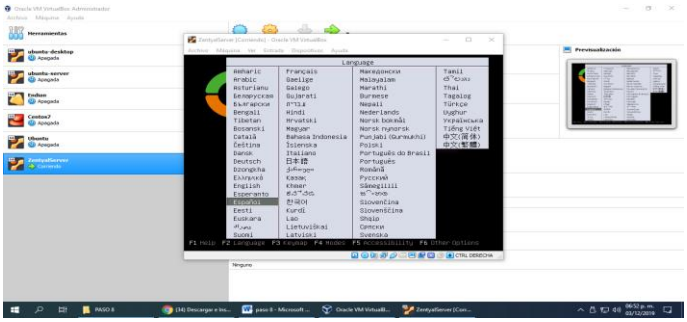

Ilustración 1. Interfaz inicial para selección de idioma.

Se selecciona la primera opción de instalación que es la

de desarrollo:

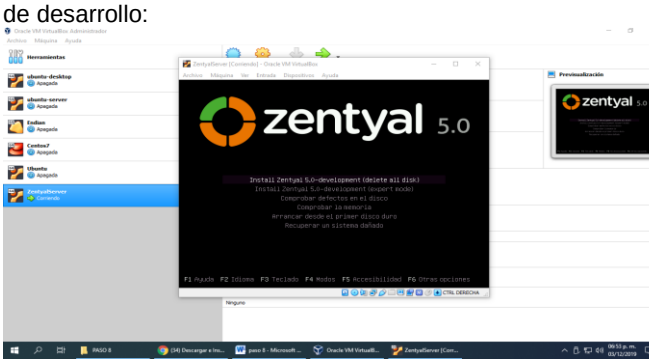

Ilustración 2. Menú de instalación de Zentyal.

Se seleccionan opciones para el idioma, ubicación, teclado y distribución de teclado:

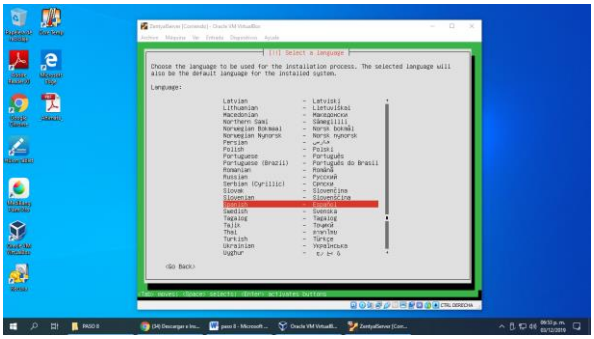

Ilustración 3. Selección de Lenguaje.

Se configura la red, estableciendo la interfaz de red primaria:

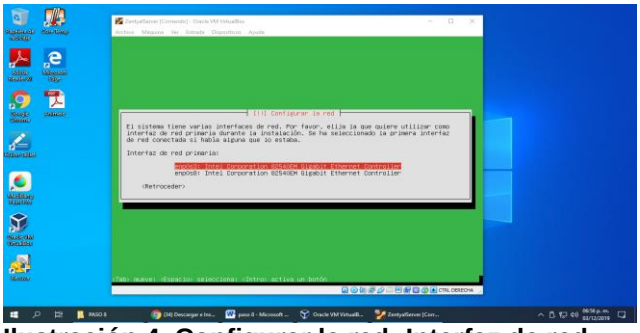

Ilustración 4. Configurar la red- Interfaz de red primaria.

Se configuran parámetros para nombre de equipo, usuario y clave de ingreso:

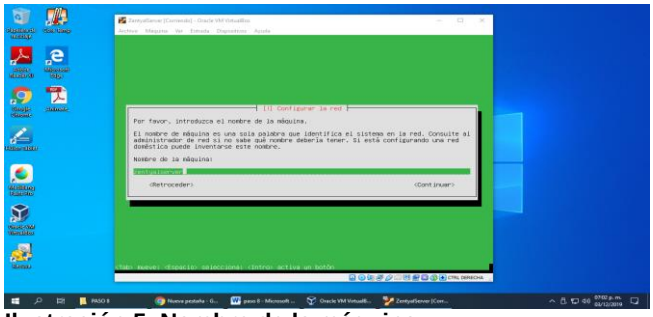

Ilustración 5. Nombre de la máquina.

Se instala todo el sistema de archivos del sistema:

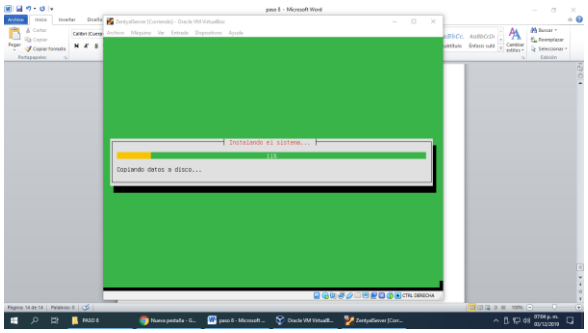

Ilustración 6. Instalación del sistema.

Al finalizar la instalación, se debe reiniciar el equipo.

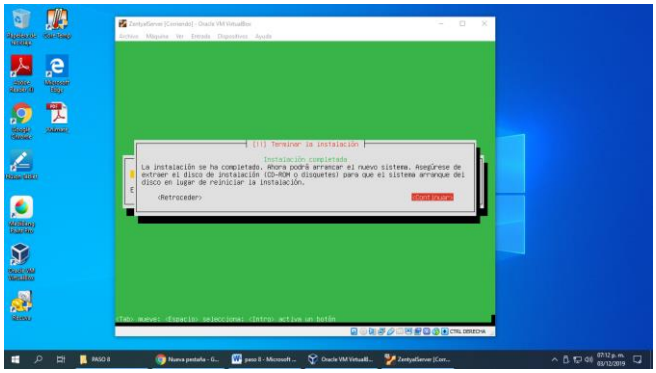

Ilustración 7. Instalación Completada.

2.4 Ingreso a Zentyal Server

Una vez reinicie el sistema, automáticamente ingresa a la interfaz web de administración de Zentyal, ingresando previamente las credenciales de acceso:

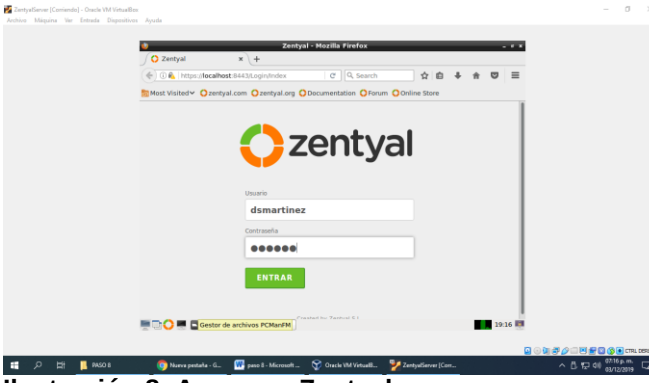

Ilustración 8. Acceso a Zentyal.

2.5 Configuración inicial

Se debe realizar una configuración inicial al empezar Zentyal, como la instalación de paquetes y la configuración de interfaces de red:

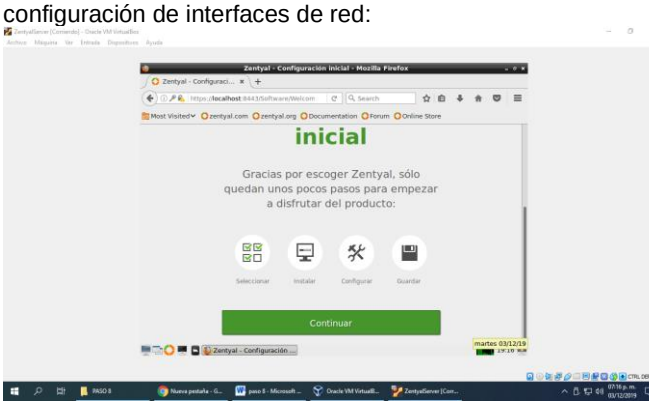

Ilustración 9. Configuración inicial Para Zentyal.

Se definen los tipos de interfaces externa e interna del servidor y también el direccionamiento IP y redes para cada interfaz:

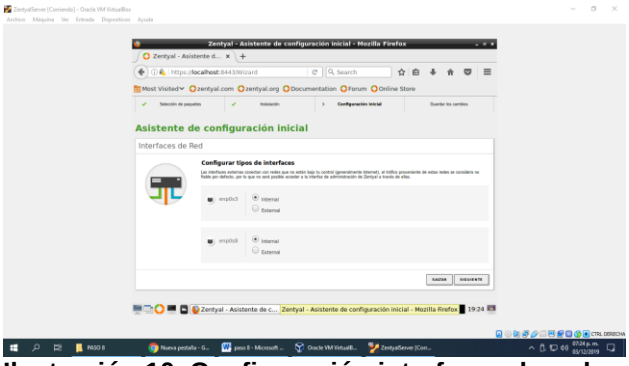

Ilustración 10. Configuración interfaces de red.

Después de realizar la configuración inicial y guardar los cambios, se accede al Dashboard, que es la interfaz principal de la aplicación Web.

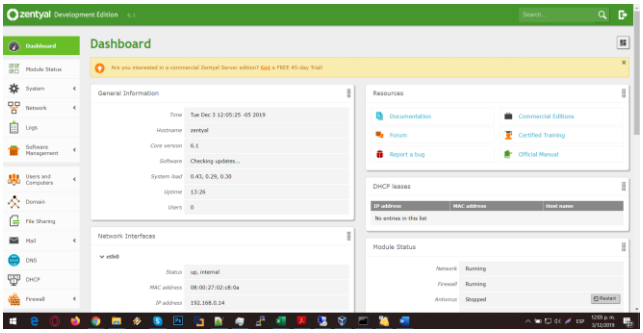

Ilustración 11. Dashboard en Zentyal.

3 Temáticas planteadas

Se plantean a continuación 5 temáticas con la configuración y puesta en marcha de varios servicios de red sobre Zentyal server.

Se tiene en cuenta que previamente se hace la instalación de equipos cliente con Sistema Operativo Ubuntu, dentro de la misma red del servidor para la aplicación de los diferentes servicios red configurados en Zentyal.

Las temáticas se muestran a continuación en la Tabla 1:

Tabla 1. Temáticas

Temática	Descripción
1	DHCP Server, DNS Server y Controlador de Dominio
2	Proxy no transparente
3	Cortafuegos
4	File Server
5	VPN

3.1 Temática #1: DHCP Server, DNS Server y controlador de dominio

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

Configuración de DHCP server

En el estado de los módulos chequeamos el DHCP y lo activamos

Escogemos la opción de configuración para empezar con el servicio

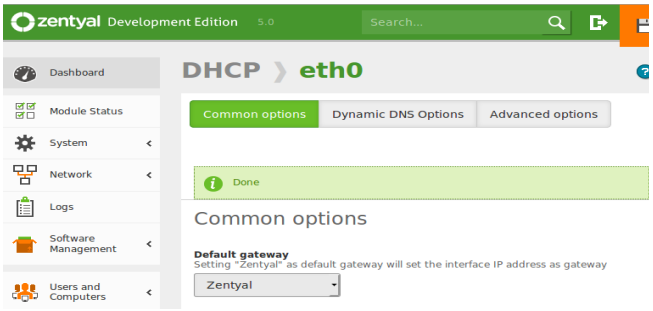

Ilustración 12. Configuración de DHCP server

Después de ver los rangos disponibles, establecemos nuestro propio rango para DHCP

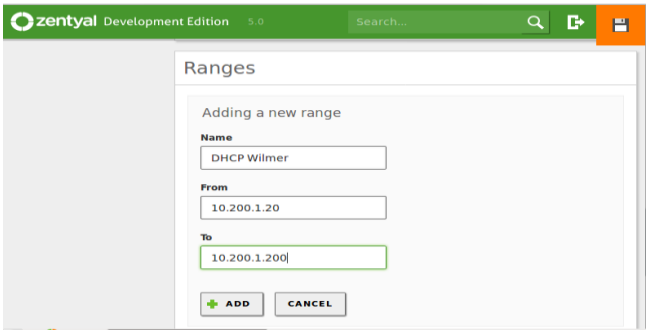

Ilustración 13. Rango de ip para DHCP

Notamos como está conectado el primer cliente DHCP, estando en la misma red.

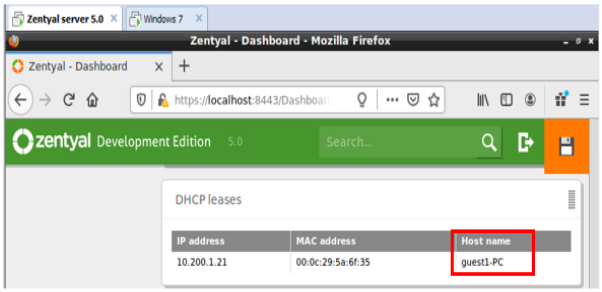

Ilustración 14. Cliente conectado por DHCP

Configuración de servidor DNS.

Habilitamos DNS en el estado de módulos

Nos vamos al módulo del DNS y creamos nuestro nombre de dominio, lo cual ya habíamos configurado en la instalación del servicio.

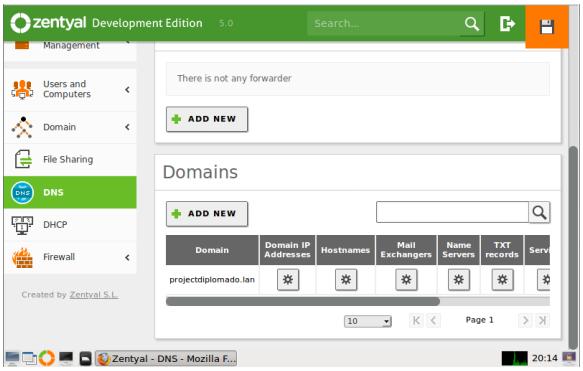

Ilustración 15. Nombre de Dominios

Configuramos el servicio de DHCP para que integre nuestro DNS en pool de direcciones o en su configuración.

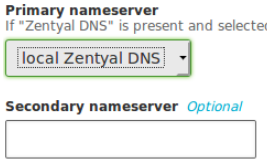

Ilustración 16. Integración del DNS

Se realiza un nslookup en el equipo cliente e identificamos como aparece nuestro dns, con el nombre del server como alias.

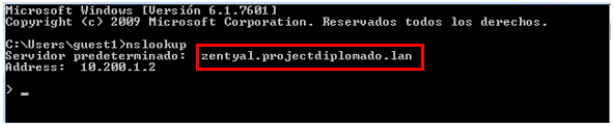

Ilustración 17. Nslookup en el cliente

En los hosts names agregamos un alias www por si queremos agregar una intranet o una página web.

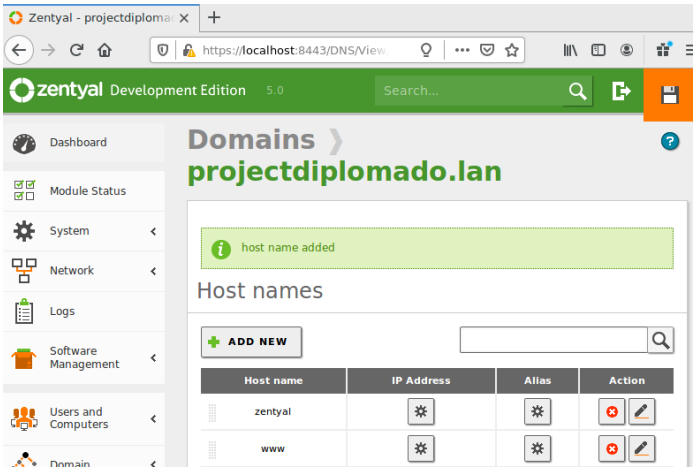

Ilustración 18. Alias agregado al host names

Agregamos el alias en los nombres del servidor.

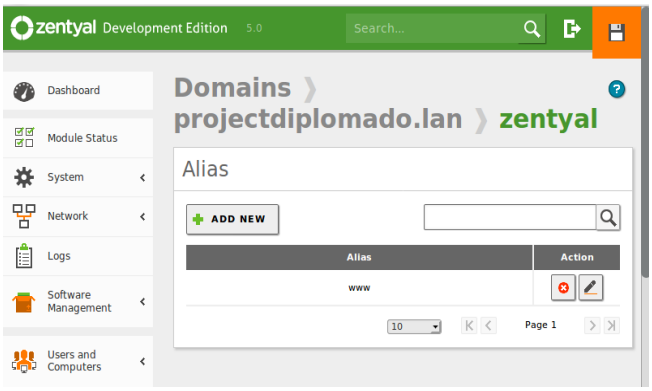

Ilustración 19. Alias en los nombres del servidor

DHCP cliente Ubuntu

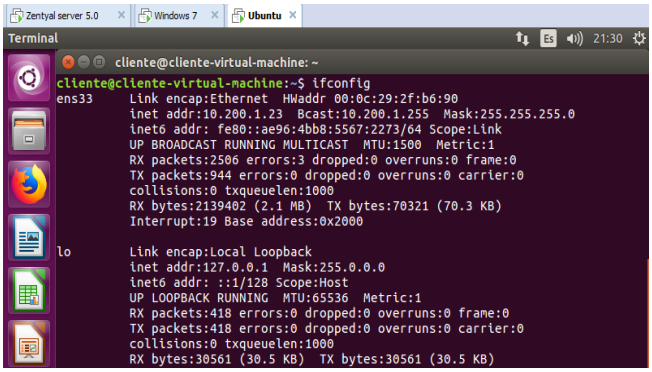

Ilustración 20. Equipo cliente

Aplicación de nslookup en cliente Ubuntu

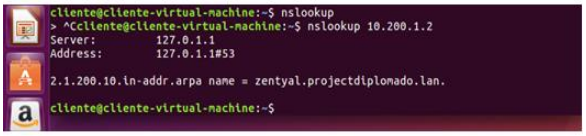

Ilustración 21. Nslookup en cliente ubuntu

Configuración de directorio activo

Anteriormente instalamos los paquetes a utilizar, estos son los paquetes que instala el domain controller. Dejamos la configuración por defecto

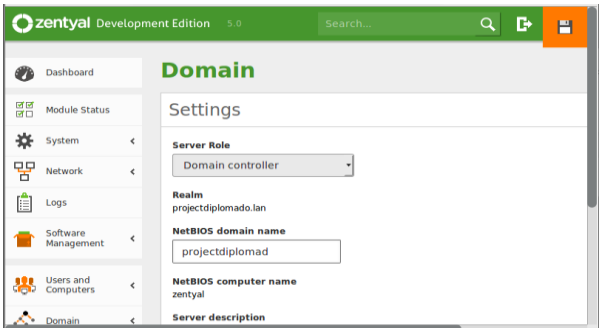

Ilustración 22. Paquete de controlador de dominios

Procedemos agregando un nuevo usuario al dominio.

Ilustración 23. Usuario nuevo al dominio

Agregar un cliente Windows al dominio, ingresamos a las propiedades del sistema en Windows, Ahora seleccionamos configuración avanzada del sistema

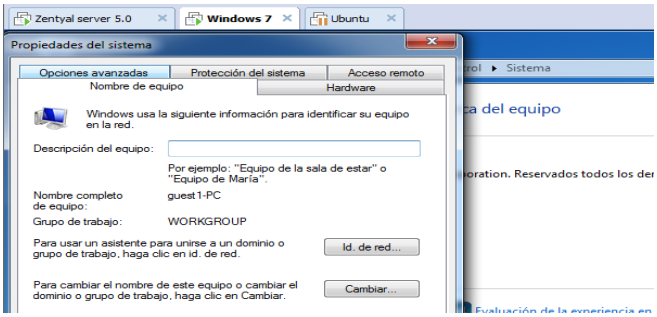

Ilustración 24. Agregar cliente al dominio

Nos situamos en la pestaña nombre de equipo y damos clic en cambiar.

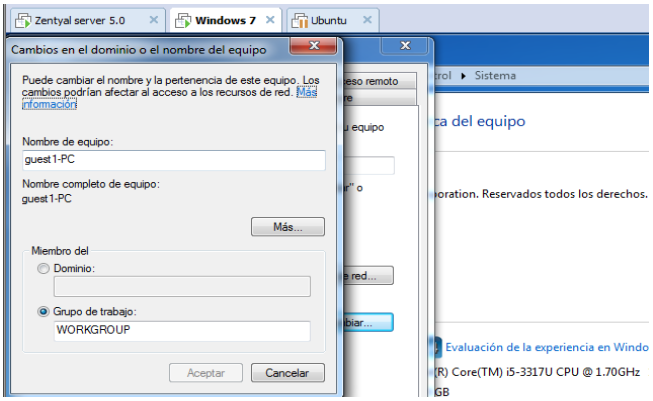

Ilustración 25. Nombre del equipo

Seleccionamos dominio y procedemos a escribir el nuestro.

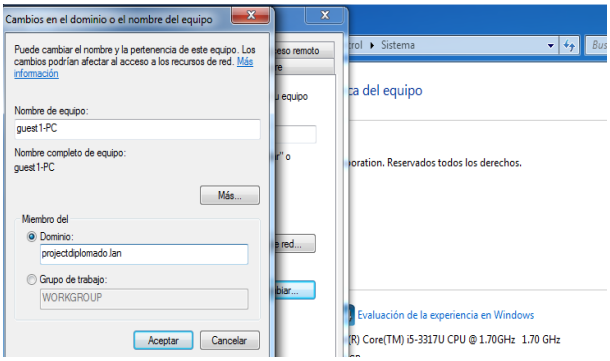

Ilustración 26. Cambios en el dominio del equipo

Se nos despliega una comprobación de usuario, escribimos las credenciales del nuestro usuario ya que hace parte del grupo administrador.
Luego iniciamos sesión.

Agregar cliente Linux al dominio

Se instala los repositorios o paquetes para el proceso

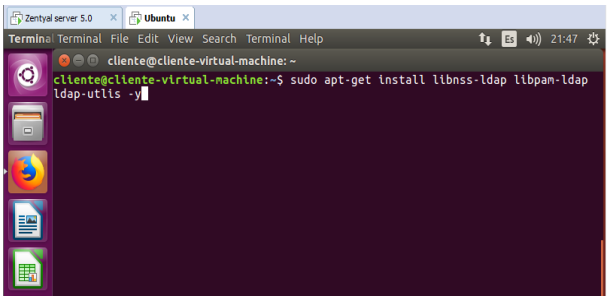

Ilustración 27. Instalación de paquetes

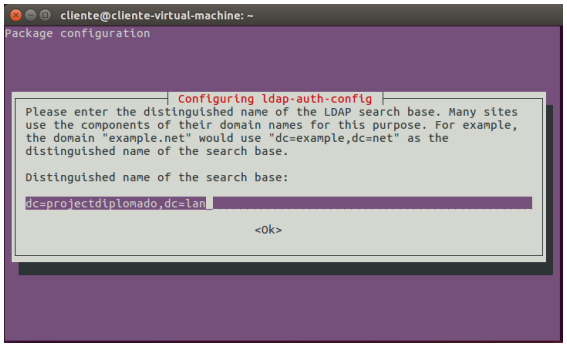

Ilustración 28. Configuración del paquete a instalar

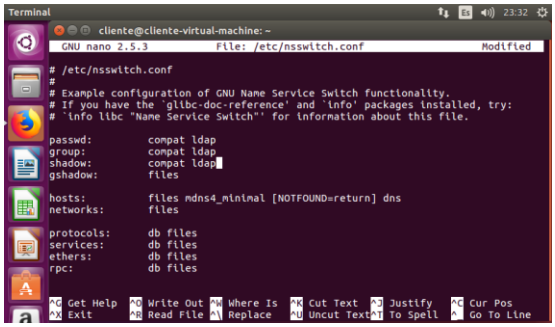

Ilustración 29. Edición de archivo nsswitch.conf

Después se editan tres archivos adiciones se reinicia y se inicia sesión con el usuario.

3.2 Temática #2: Proxy no transparente

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

Configuramos las interfaces de red.

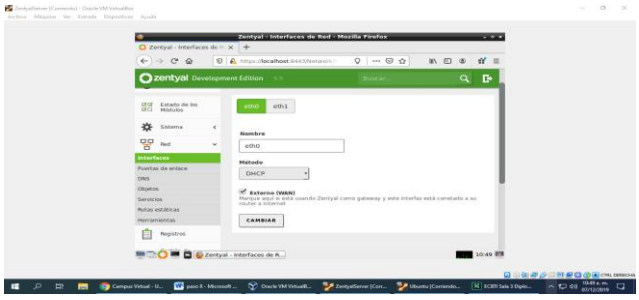

Ilustración 30. Interfaz de red eth0

La eth0 será la interfaz wan y su método será DHCP, la interfaz eth1 se configura en modo estático y se le asigna la IP 192.168.10.1 para conectar los clientes.

Desde la sección de módulos se activa el HTTP Proxy.

Los equipos clientes se deben configurar con direcciones IP fijas y con la puerta de enlace apuntando a Zentyal para que todo el tráfico pase por allí.

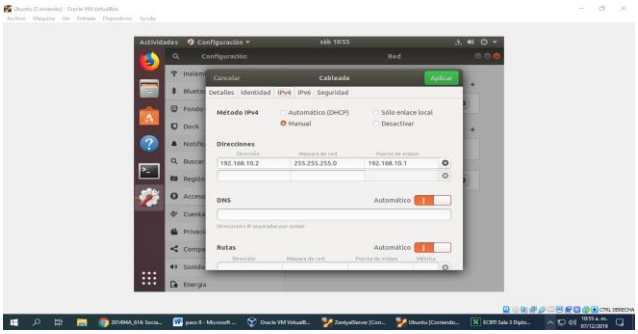

Ilustración 31. Configuración de ip de equipo cliente

En la sección de Red/objetos se añade un nuevo objeto, en este caso el equipo cliente Ubuntu, se selecciona CIDR para un solo equipo y se le indica la dirección IP del cliente.

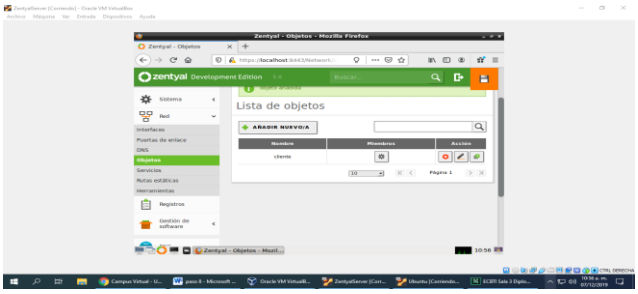

Ilustración 32. Lista de objetos de red

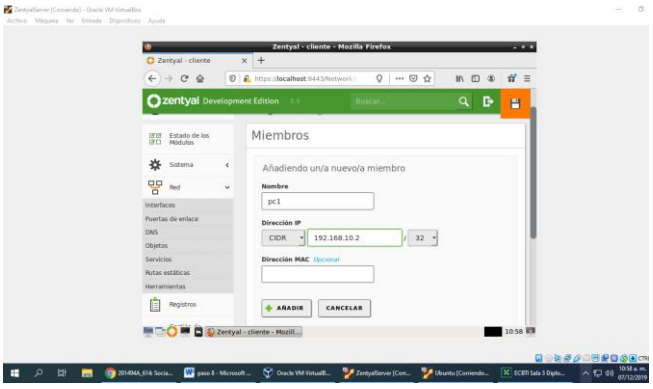

Ilustración 33. Miembros de los objetos de red

En la sección de HTTP Proxy se ingresa a los ajustes generales y se configura el servidor proxy, puerto, cache y si va a ser transparente o no.

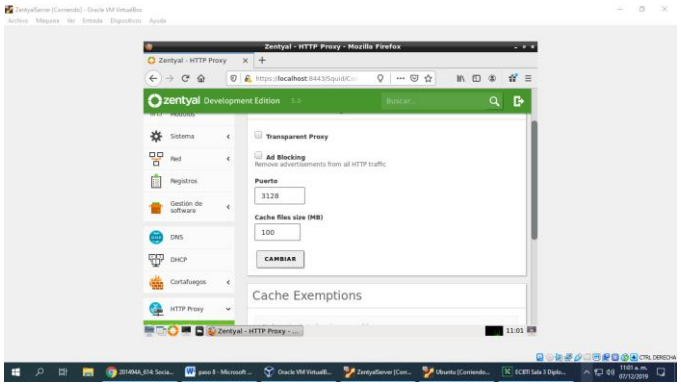

Ilustración 34. Configuraciones generales del proxy

En la sección de reglas de acceso del servidor proxy, se crea una nueva regla y en el origen se selecciona el objeto creado anteriormente y en decisión seleccionamos denegar a todos.

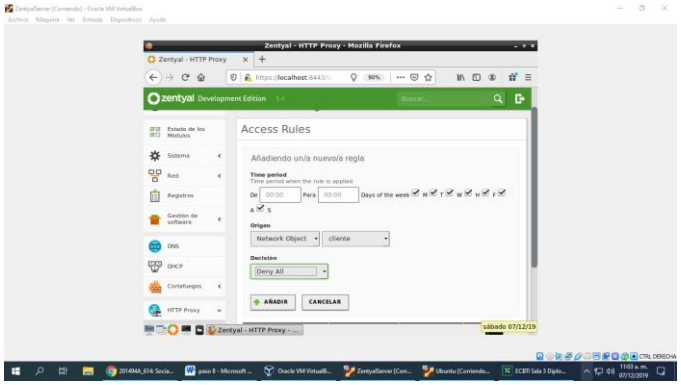

Ilustración 35. Reglas de acceso

Al final se guardan todos los cambios realizados para que surja efecto. En el navegador del cliente asignamos la dirección IP y el puerto del servidor proxy.

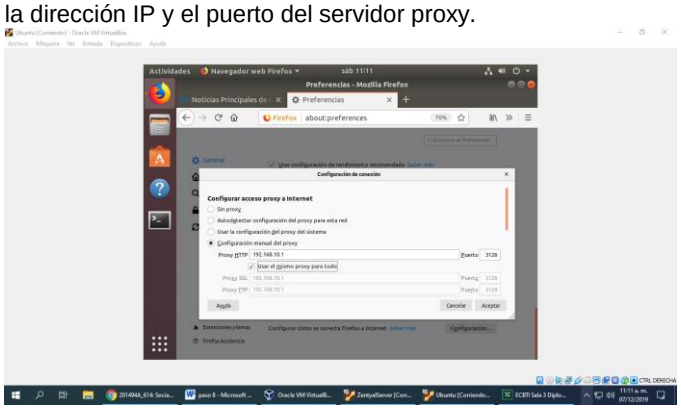

Ilustración 36. Configuración de red en el navegador

Resultados Obtenidos: En el equipo cliente (Ubuntu) se intenta ingresar a una página de internet en este caso YouTube y se evidencia claramente la restricción que le

está dando el servidor proxy desde Zentyal.

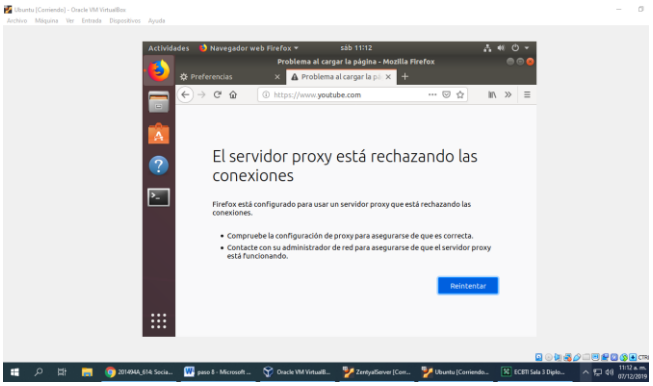

Ilustración 37. Página web bloqueada por proxy

Restricción con perfiles de usuarios.
Creación de perfiles de filtro.
Vamos al menú HTTP Proxy y damos clic en la opción filter profiles. Creamos el perfil Redes_Sociales el cual va a denegar la conexión a Facebook y YouTube.

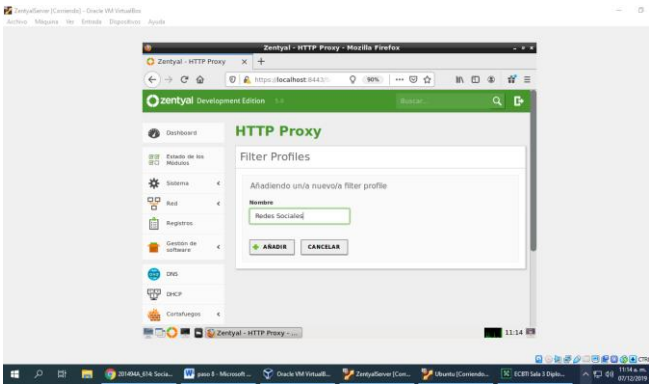

Ilustración 38. Perfiles de filtro

Vamos a la pestaña Domains and URLs para agregar los dominios que van a ser bloqueados. En nuestro caso serán facebook.com y youtube.com

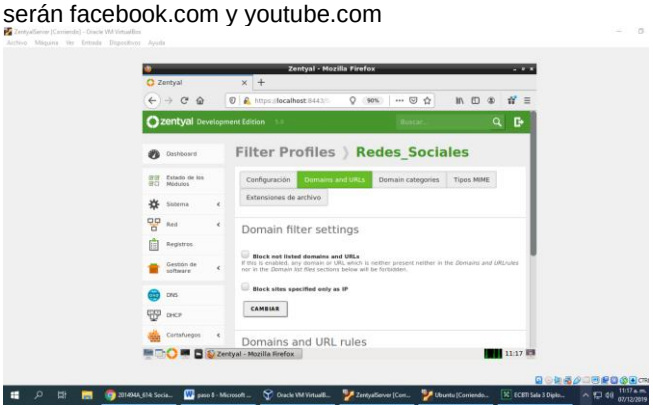

Ilustración 39. Dominios y URLs a bloquear

Vamos a aplicar el perfil creado. En el menú HTTP Proxy vamos a la opción Access Rules. Añadimos una nueva regla de acceso, el origen será el cliente es decir el objeto de red creado anteriormente, en decisión seleccionamos Apply Filter Profile y seleccionamos el perfil creado. Damos clic en cambiar y guardamos los cambios.

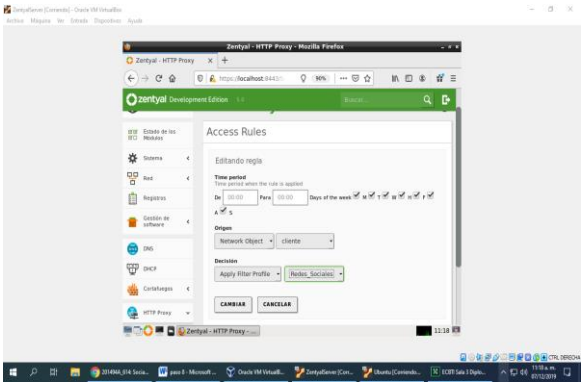

Ilustración 40. Aplicación de filtro creado

Vamos al navegador web del equipo cliente y tratamos de ingresar a facebook.com, no podemos acceder ya que el servidor proxy está rechazando la conexión.

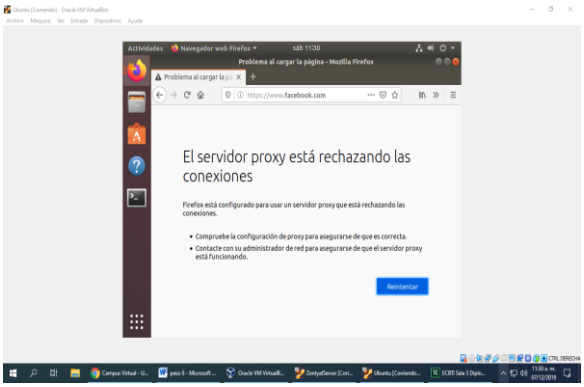

Ilustración 41. Página web bloqueada por proxy

Pero si podemos ingresar a una página o portal web diferente, ingresamos a la página web de la UNAD y podemos observar que hay acceso a ésta.

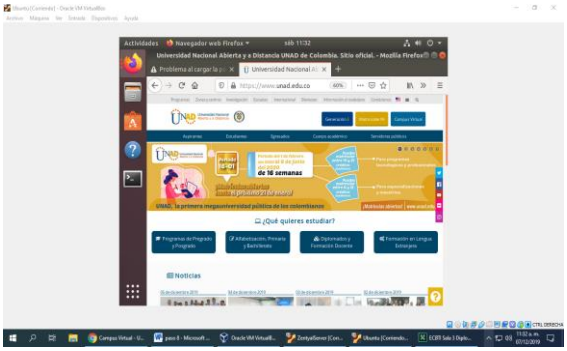

Ilustración 42. Página web permitida

3.3 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.

Para poder realizar la configuración de nuestros cortafuegos primero debemos configurar la red de nuestro servidor zentyal y lo realizaremos realizando la configuración del DHCP, Protocolo de configuración dinámica de Host. Anteriormente habíamos configurado la ip y la máscara de red con lo cual tenemos un rango de 8 bits para la red con lo cual tenemos disponibles desde 1 a 254 ips y podremos configurar nuestro DHCP.

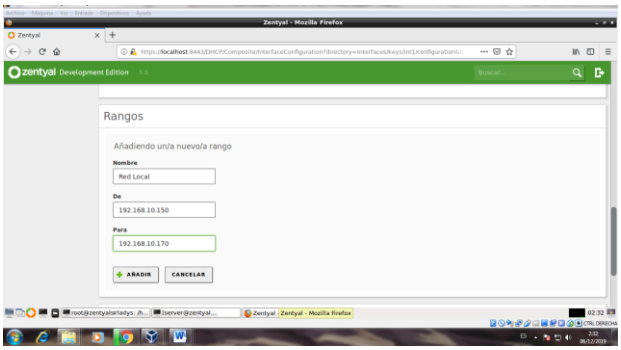

Ilustración 43. Nuevo rango de ips

Después de realizar la configuración del servicio DHCP, procedemos a iniciar la maquina Ubuntu cliente para verificar que se encuentre funcionando nuestro servicio y que se puede conectar a nuestro servidor zentyal.

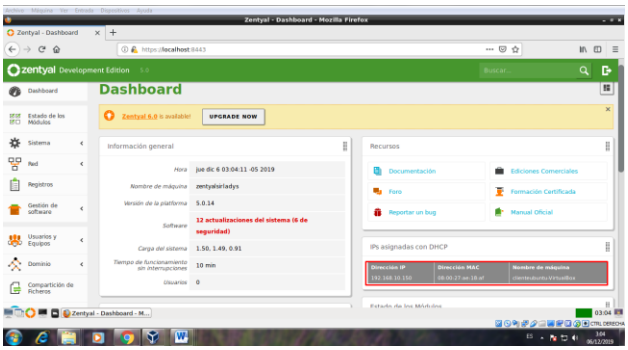

Ilustración 44. Interfaz de zentyal

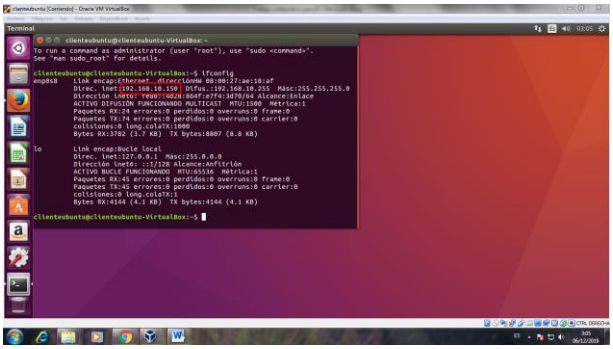

Ilustración 45. Dirección ip equipo cliente

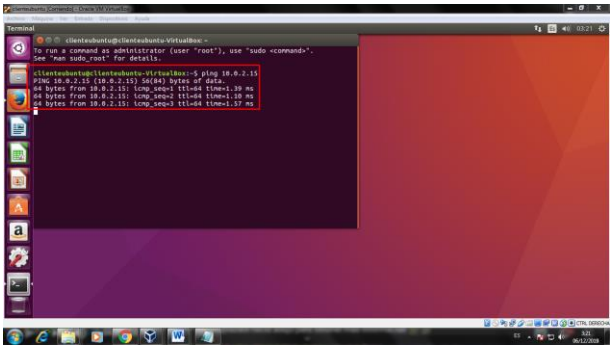

Ilustración 46. Ping a zentyal

Procederemos a realizar la configuración del cortafuego o firewall en nuestro servidor zentyal y su respectiva comprobación en el cliente Ubuntu.

Procedemos a comprobar en nuestro cliente Ubuntu la conexión a internet.

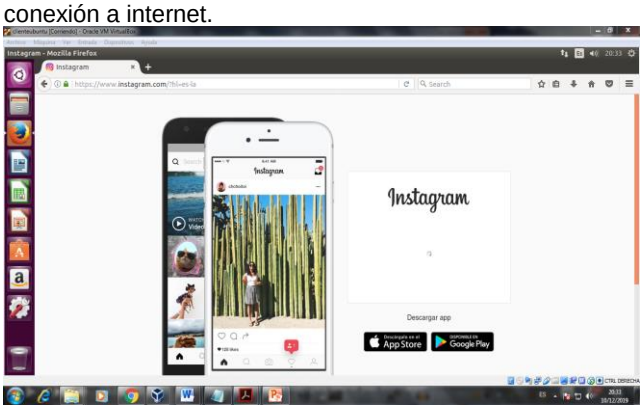

Ilustración 47. Prueba conexión a internet en el cliente

Realizamos la configuración del firewall para la red LAN que hemos creado. Para el desarrollo de esta temática realizaremos el bloqueo de la red social Facebook para lo cual debemos configurar el cortafuegos de tal manera que bloquee el protocolo https y debemos de tener todas las ip que tiene asignadas el dominio Facebook.com. Estas direcciones ips o rangos las podemos encontrar

en las siguientes direcciones web:
https://awebanalysis.com/es/ipv4-as-name-directory/Facebook-comma-+Inc./
https://ipinfo.io/AS32934?fbclid=IwAR0XddlTY4dydYM2DjB_PFsMt9-xdMTQisOkmJ2Lx8pcVaNXT_5I9_WystY

Teniendo claro las direcciones ip que vamos a aplicar las reglas y políticas del cortafuegos de zentyal, empezando por crear un objeto de red en donde podemos agregar todas las CIDR (Ruteo interno de dominios sin clases) es un estándar de red para la interpretación de direcciones IP.

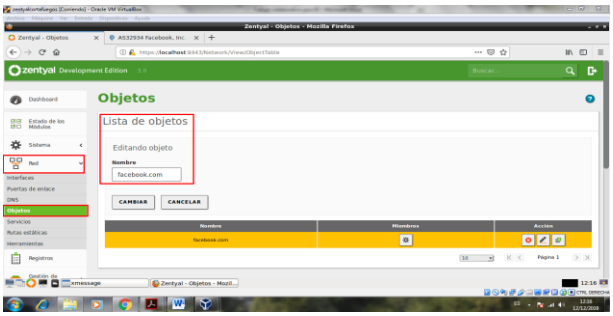

Ilustración 48. Listas de objetos de red

Agregamos cada uno de los miembros que compone nuestro objeto.

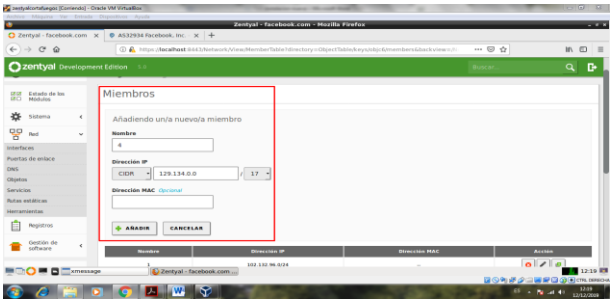

Ilustración 49. Miembros de objetos de red

Guardamos cambios después de agregar todas los CIDR.

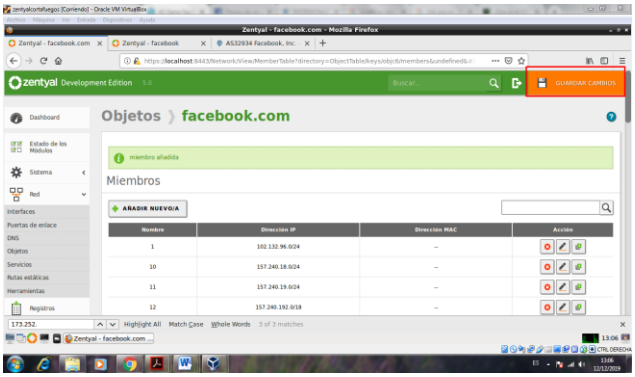

Ilustración 50. CIDR agregados

Procedemos a realizar la configuración de las reglas y políticas del cortafuego. Reglas de filtrado para redes internas.

Ilustración 51. Reglas de filtrado

Ilustración 52. Configuración de reglas

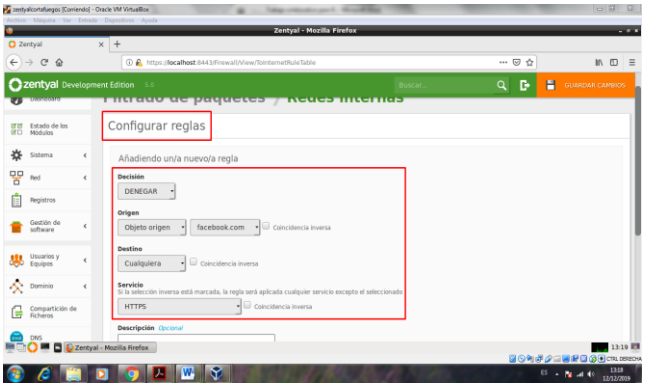

Ilustración 53. Configuración de reglas aplicadas

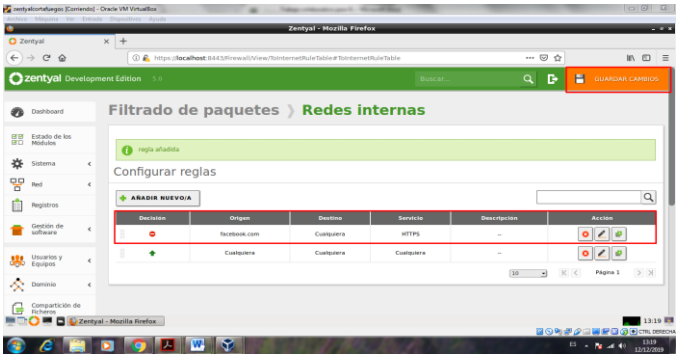

Ilustración 54. Reglas creadas y aplicadas

Ya quedan guardados los cambios de las configuraciones realizadas y podemos proceder a realizar la comprobación del bloqueo de la web Facebook.

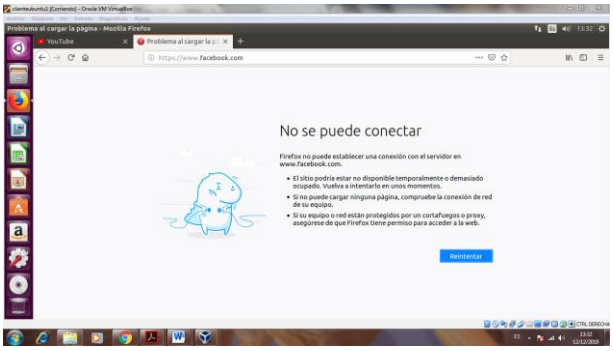

Ilustración 55. Bloqueo de sitio web

Acceso a otras páginas.

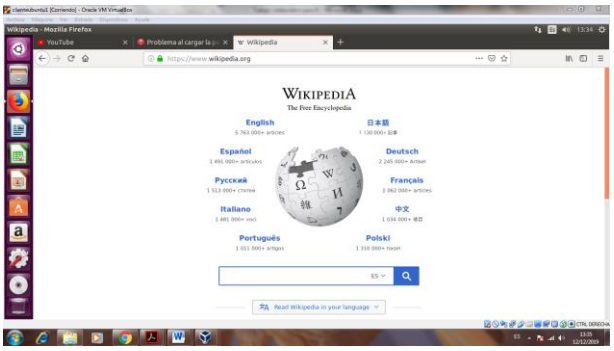

Ilustración 56. Sitio web permitido

3.4 Temática #4: File Server y Print Server

Para configurar el servidor de archivos, nos dirigimos al menú “Compartición de ficheros” y creamos una nueva conexión.

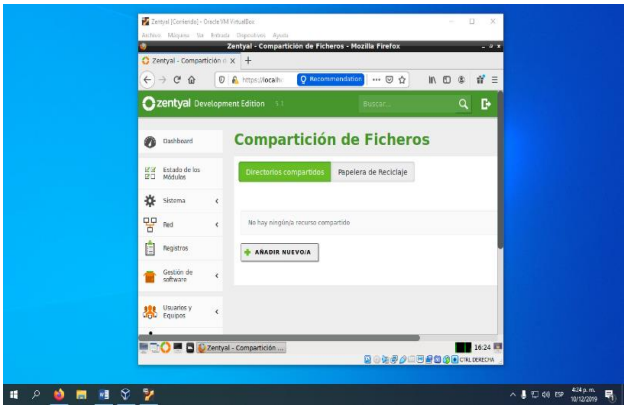

Ilustración 57. Menú compartición de ficheros

Creamos el nuevo recurso compartido con el nombre de archivos y compartiremos la ruta con el mismo nombre dentro del directorio de Zentyal.

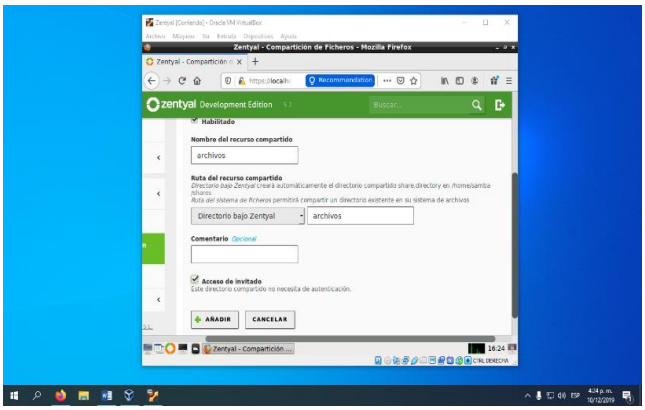

Ilustración 58. Creación del recurso compartido

Nos vamos a la configuración del recurso y le damos permisos tanto de lectura como escritura a los usuarios del dominio.

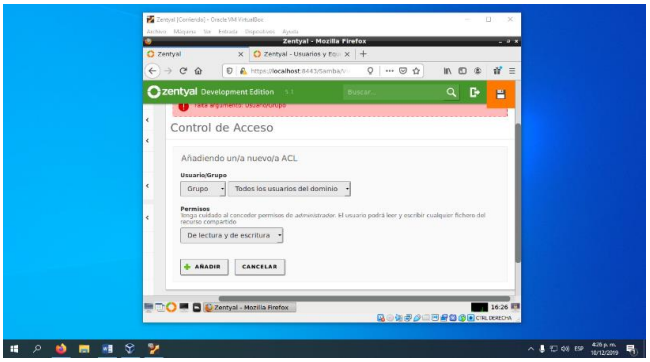

Ilustración 59. Configuración del recurso

Guardamos los cambios en el botón de disquete situado en la esquina superior derecha de la ventana y ya estaremos listos para realizar la conexión.

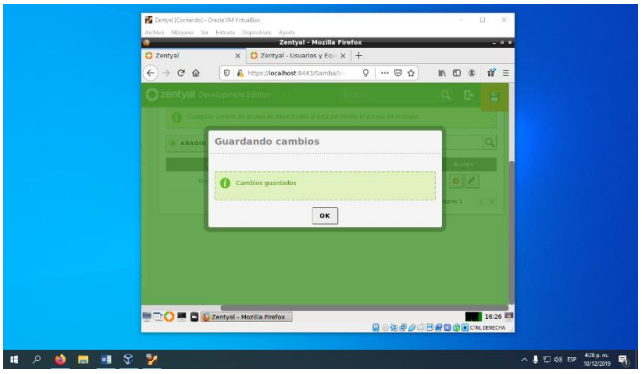

Ilustración 60. Cambios guardados

Es necesario identificar la dirección IP de la máquina virtual por lo que utilizaremos el comando ifconfig para obtener la dirección que utilizaremos en el explorador de archivos de Windows.

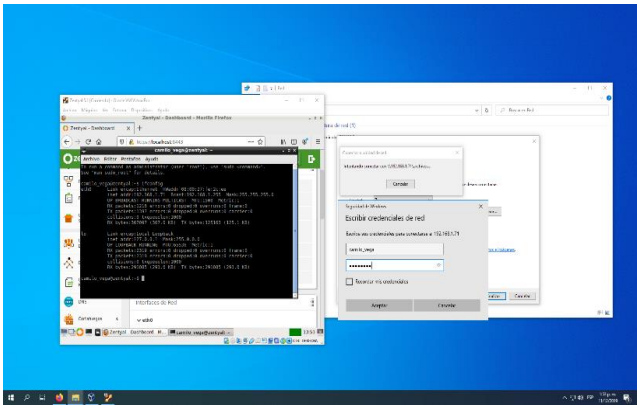

Ilustración 61. Ip del equipo cliente

Una vez digitadas las credenciales del usuario, tendremos acceso remoto desde el explorador de archivos de Windows a la carpeta del servidor de Zentyal.

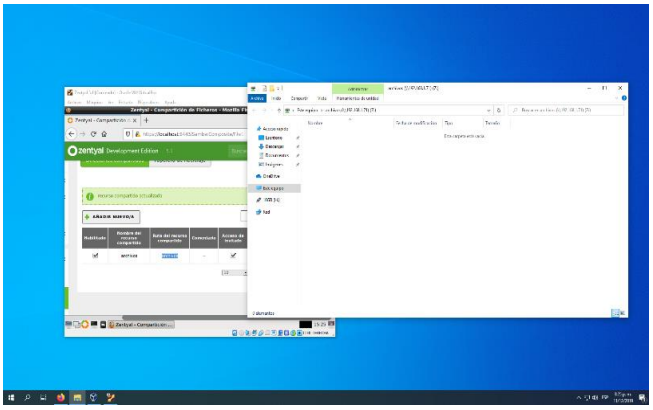

Ilustración 62. Acceso remoto del cliente al servidor

3.5 Temática #5: VPN

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

Ingresamos a Zentyal y realizaremos los pasos para la creación y configuración de VPN

Vamos a la opción Certification Authory → General

Ilustración 63. Certificados

Se crea el certificado CA-Zentyal y clic en botón create

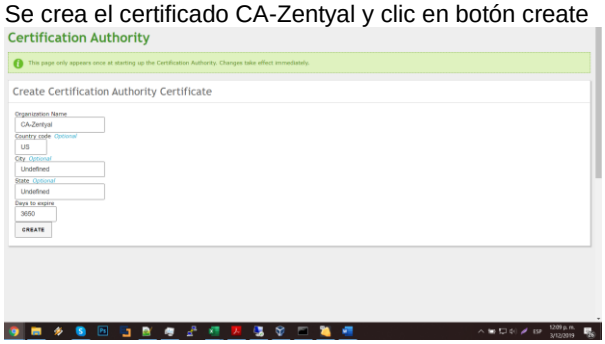

Ilustración 64. Creación de certificado CA-Zentyal

3.5.1 Añadir servidor VPN

Vamos VPN → Servers

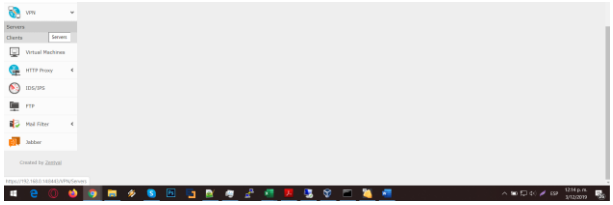

Ilustración 65. Módulo VPN

Clic en ADD NEW

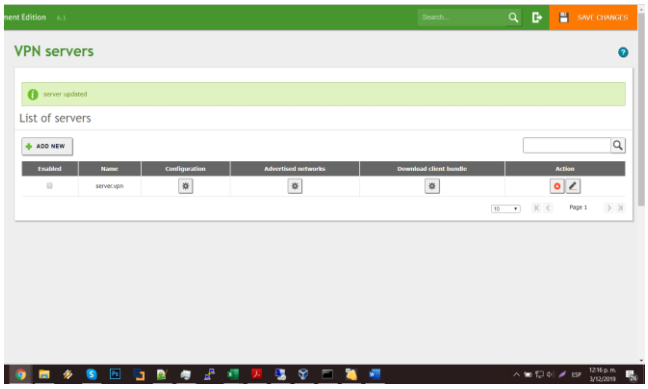

Ilustración 66. Lista de servidores

3.5.2 Creación de Certificado para VPN

Vamos a la opción Certification Authoty → General

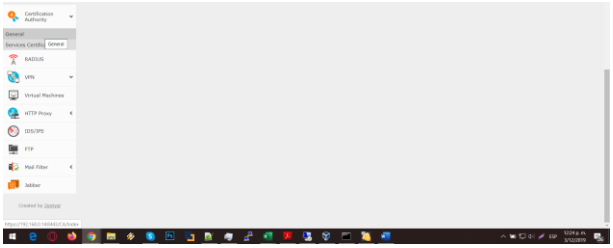

Ilustración 67. Creación de certificado CA

Adicionamos el certificado y le damos clic en ISSUE

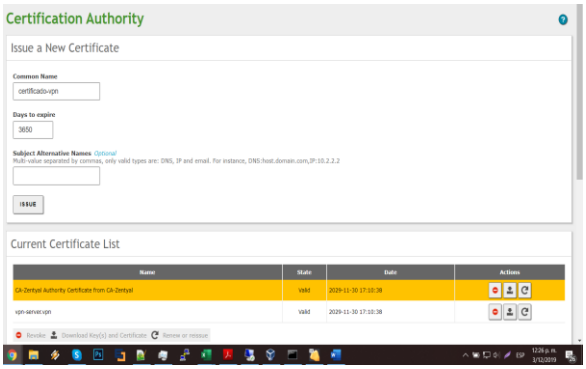

Ilustración 68. Certificado CA creado

Y el CA queda creado

3.5.3 Configuración de servidor VPN

Vamos a la opción de VPN → Servers y damos clic en configure.

Y validamos que VPN address 192.168.160.0 / 24 y en server certificate seleccionamos el certificado que creamos (certificado-vpn), activamos la opción TUN interface y clic en CHANGE.

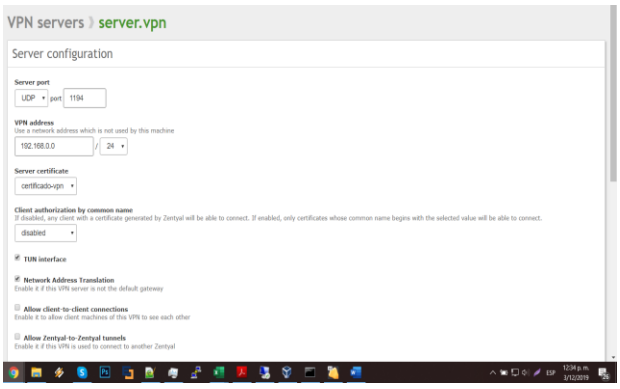

Ilustración 69. Selección del certificado creado

3.5.4 Configuración de Servicios

Vamos network → services

Clic en ADD NEW y lo llamamos red-vpn

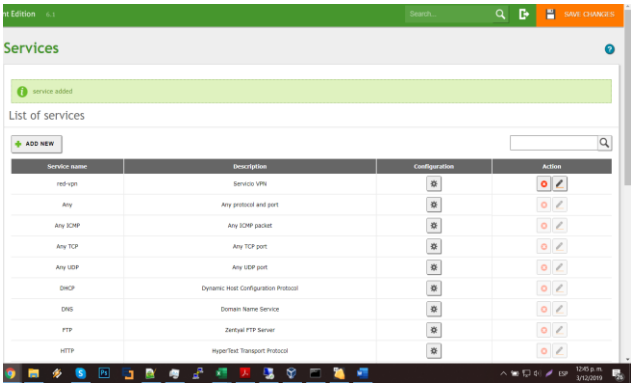

Ilustración 70. Lista de servidores de red

En Protocolo seleccionamos UDP, en source port Any, Destination Port seleccionamos Single port y el puerto 1194. Clic en ADD.

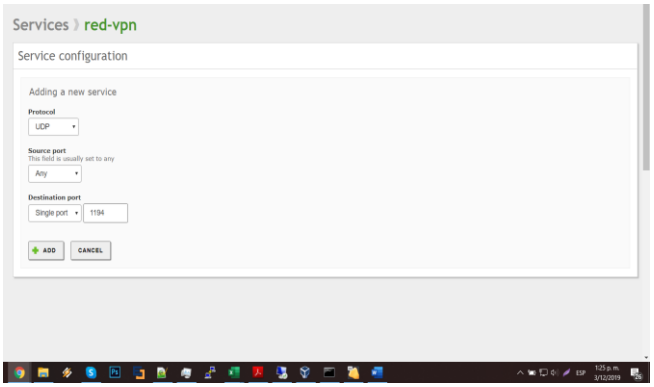

Ilustración 71. Configuración de servicios

3.5.5 Descargar VPN Client

Vamos a la opción de VPN Servers y clic en configure

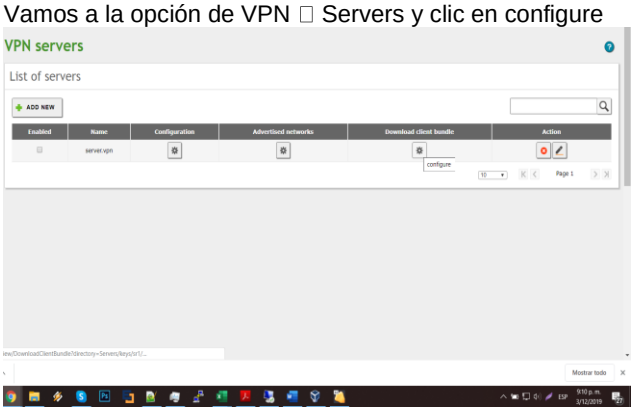

Ilustración 72. Lista de servidores VPN

Y configuramos y clic en download

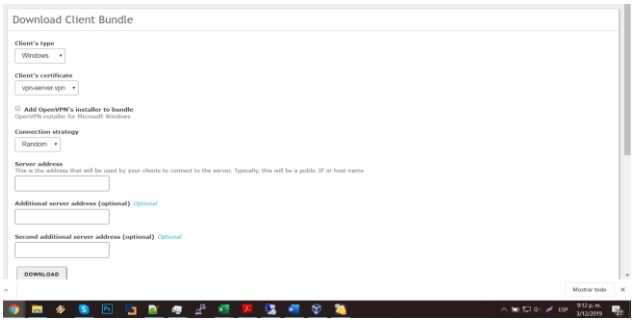

Ilustración 73. Descarga del servidor VPN

Ilustración 74. Lista de servidores VPN

3.5.6 Pruebas de VPN

La prueba de VPN configurado se va a realizar entre el servidor Zentyal y la maquina Windows, debido al poco hardware disponible. Se realiza la descarga de los certificados

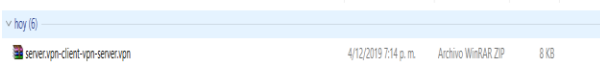

Ilustración 75. Servidor VPN descargado

Luego se descarga el software OpenVpn para Windows y lo instalamos.

Sobre OpenVpn GUI le damos clic derecho importar

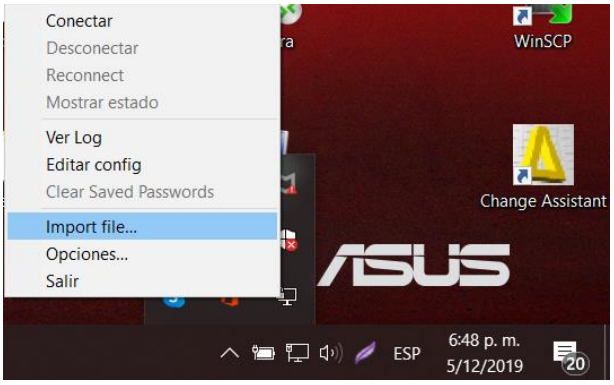

Ilustración 76. Importación de certificado a OpenVpn

Y buscamos la ruta donde descomprimimos el certificado que descargamos

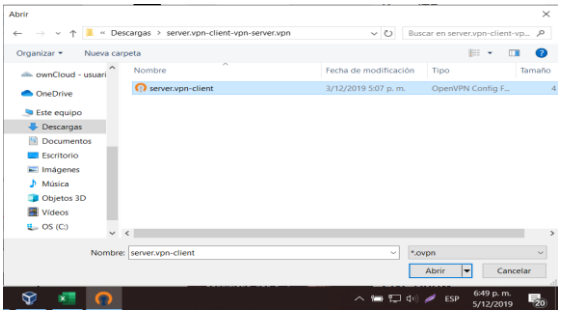

Ilustración 77. Certificado descargado

Clic en aceptar. Importante que los archivos descomprimidos estén en C:\Users\sic\OpenVPN\config\server.vpn-client para este caso.

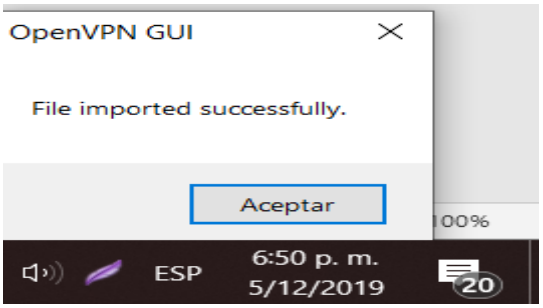

Ilustración 78. Archivo importado exitosamente

Luego le damos clic izquierdo en OpenVPN GUI y seleccionamos el certificado y le damos clic en conectar

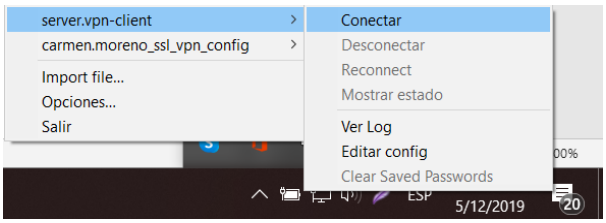

Ilustración 79. Conectar al servidor VPN

Cuando está conectado nos asigna una IUP en este caso nos asignó la 192.168.160.6

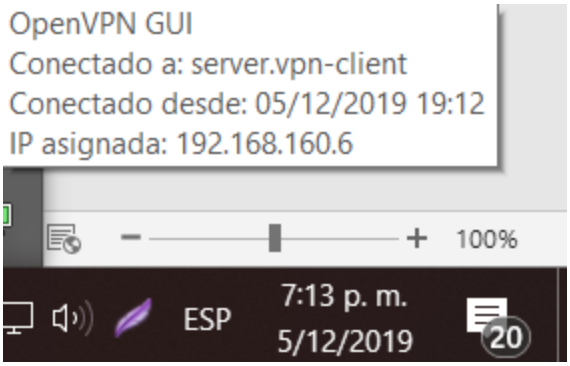

Ilustración 80. Ip asignada al equipo cliente

Con telnet de Windows conectamos con la ip 192.168.160.6 puerto 21 que es el FTP de Zentyal

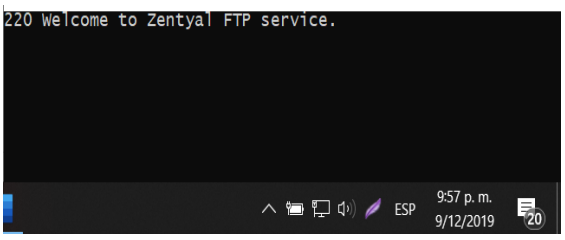

Ilustración 81. Conexión del cliente al servidor VPN

4. CONCLUSIONES

Se ha adquirido conocimiento respecto a los servicios ofrecidos por Zentyal 5.0 y sus componentes más importantes como los es DHCP, DNS y servidor de Dominio ofreciendo a la sociedad un profesional con altas características de manejo de los componentes de Linux.

En esta evidencia pudimos implementar a través de la solución en Zentyal un proxy no transparente capaz de controlar (bloquear) el acceso a internet o a ciertas páginas y portales web que podrían afectar de manera significativa el rendimiento y la productividad de las personas en un ambiente de trabajo.

Es gratificante trabajar con este tipo de distribuciones el cual este sis tema operativo de diseño ingenioso, gratuito y tiene unos estándares que manifiestan su eficacia que permite que este sistema sea uno completo y fácil de manipular.

Al final pudimos comprobar su funcionalidad a nivel medio como lo es el bloqueo de páginas de redes sociales como facebook y YouTube y cómo podemos mantener ese tipo de seguridad en lo que hacemos.

El cómo implementar Zentyal permite una mejor estructura de seguridad sobre conexión a equipos remoto con VPN. Reconocer la importancia de herramientas como Zentyal para la administración de infraestructura.

5. REFERENCIAS

[1] Ricardo Rodriguez, (29 mayo 2015). Configuración y conexión a un servidor VPN con Zentyal usando OpenVPN, archivo [VIDEO], recuperado de: https://www.youtube.com/watch?v=3rNfipxE-9o

[2] Zentyal para administradores de redes, (s.f). Zentyal para administradores de redes, archivo [PDF]. Recuperado de: https://zentyal.com/wp-content/themes/storefront-zentyal-child/assets/files/sample_chapter_zentyal_vpn_openvpn_es.pdf

[3] Jair Gómez Arias. [JGAITPro]. (2014, mayo 7). Zentyal - Instalar y configurar Proxy Web HTTP Trasparente. Recuperado de: https://www.youtube.com/watch?v=X54YKfeFQhQ

[4] Jair Gómez Arias. [JGAITPro]. (2014, mayo 20). Zentyal - Configurar Proxy Web HTTP No Transparente. Recuperado de https://www.youtube.com/watch?v=PG7pcYmBkw4

[5] Sanz, M. P. (2008). Seguridad en Linux: Guía práctica. (Páginas. 60 - 76). Recuperado de https://ebookcentral-proquest-com.bibliotecavirtual.unad.edu.co/lib/unadsp/reader.action?docID=3218549&ppg=68

[6] Singh, A. (2013). Instant Kali Linux. (Páginas. 1 - 48). Birmingham [UK]: Packt Publishing. Recuperado de http://bibliotecavirtual.unad.edu.co/login?url=https://search-ebscohost-com.bibliotecavirtual.unad.edu.co/login.aspx?direct=true&db=e000xww&AN=656227&lang=es&site=ehost-live&ebv=EB&ppid=pp_1

[7] Muhammad Arifin, F., Andriana Mutiara, G., & Ismail, I. (2017). Implementation of Management and Network Security Using Endian UTM Firewall. (Páginas. 1 - 9). Recuperado de http://bibliotecavirtual.unad.edu.co/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=edsbas&AN=edsbas.C2217DDD&lang=es&site=eds-live&scope=site

[8] Muniz, J., & Lakhani, A. (2013). Web Penetration Testing with Kali Linux: A Practical Guide to Implementing Penetration Testing Strategies on Websites, Web Applications, and Standard Web Protocols with Kali Linux. (Páginas. 7 – 31). Birmingham: Packt Publishing., Recuperado de http://bibliotecavirtual.unad.edu.co/login?url=https://search-ebscohost-com.bibliotecavirtual.unad.edu.co/login.aspx?direct=true&db=e000xww&AN=644345&lang=es&site=ehost-live&ebv=EB&ppid=pp_7