

Diplomado de Profundización en Linux (Opción de trabajo de grado) 201494-7 TC8. Implementación y Administración de un Servidor Zentyal

Héctor Enrique Morales Hernández - Código:80.231.371

hecenmoher@gmail.com

Iván Darío Restrepo - Código:80902659

idarior0385@gmail.com

Andrés Eduardo Ardila - Código:80.844.504

ardilandres@hotmail.com

Luis Fernando Muriel Delgado Código:80.227.496

fermunad@gmail.com

Luis Fernando Umbarila – Código:80245524

Luis@umbarila.me

Resumen— En el siguiente artículo científico se expone el proceso realizado para instalación y configuración del servidor Zentyal mediante el cual se implementan los servicios y plataformas DHCP Server, DNS Server y Controlador de Dominio, Proxy no transparente, Cortafuegos y VPN, enfocados en la administración de infraestructura de servidores.

Abstract— The following scientific article exposes the process carried out for installation and configuration of the Zentyal server through which the services and platforms DHCP Server, DNS Server and Domain Controller, Non-transparent Proxy, Firewall and VPN are implemented, focused on the management of server infrastructure

I. INTRODUCCIÓN

Tiempo atrás los administradores en un sistema computacional cuando desplegaban un servicio en un entorno empresarial, debían de realizar el mismo proceso de forma repetida en cada uno de los equipos que conformaban la red. Es así como si requerían que un nuevo usuario ingresara en un equipo debían de desplazarse hasta ese equipo configurar el perfil del usuario, anexarlo a un grupo de trabajo y de igual forma configurar manualmente los servicios que este requería. Con la evolución de los sistemas operativos surgieron los sistemas operativos cliente-servidor, en los cuales un equipo que hacía como servidor suministraba una serie de servicios que requerían un conjunto de equipos cliente.

Hoy en día existen sistemas operativos orientados hacia la infraestructura de servidores, como son la familia de Windows Server y Linux que nos ofrece una variedad de distribuciones según las necesidades y tamaño de una empresa. Es así como en la familia Linux surge Zentyal Linux Small Business Server, un sistema servidor para pequeñas y medianas empresas basado en Ubuntu y

creado en España; que provee servicios importantes a una red de computadoras como DHCP, DNS, Proxy, LDAP, File Server, Print Server, VPN, entre otros, de una forma amena por medio de módulos integrados.

III. PLANTEAMIENTO Y PROBLEMA

En el presente artículo se desarrollará el proceso de instalación y configuración de un servidor con la distribución Linux Zentyal 6.0 como sistema operativo en cual se instalará, configurará y administrará una serie de servicios que podrán ser utilizados por uno o más equipos Linux o Windows.

II. MARCO TEÓRICO

A- Zentyal Server

Zentyal está concebido para ser instalado en una máquina (real o virtual) de forma, en principio, exclusiva. Esto no impide que se pueda instalar cualquier otro servicio o aplicación adicional, (no gestionado a través de la interfaz de Zentyal), que deberá ser instalado y configurado manualmente.

Zentyal funciona sobre la distribución de GNU/Linux Ubuntu en su versión para servidores, usando siempre las ediciones LTS (Long Term Support), con cinco años de soporte.

La instalación puede realizarse de dos maneras diferentes:

- Usando el instalador de Zentyal (opción recomendada),
- Instalando Zentyal sobre una distribución Ubuntu Server Edition. (zentyal.org, 2015)

B. Diseño Zentyal Server

Zentyal (anteriormente conocido como eBox Platform) es un servidor de red unificada de código abierto que estructura un plataforma unificada orientada a PYMEs. Zentyal puede actuar gestionando la infraestructura de red, es un sistema UTM que funcionar como puerta de enlace a Internet, gestionando las amenazas de seguridad, como servidor de oficina, como servidor de comunicaciones unificadas o una combinación de estas. Además, Zentyal incluye un marco de desarrollo (un framework) para facilitar el desarrollo de nuevos servicios basados en Unix. (Ecured, s.f.)

Solucionada gran parte de las problemáticas de migración de sus

sistemas operativos, servicios y puesta en marcha de los sistemas de seguridad de la infraestructura de red, se entra en la fase final de la migración y puesta en marcha de los servicios solicitados por medio de las 5 temáticas propuestas. Servidor DHCP, DNS Y LDAP, Servidor Proxy no transparente, Cortafuegos, File Server y Print Server y VPN, que serán implementados por medio de GNU/Linux Zentyal Server como sistema operativo base.

IV INSTALACIÓN DEL S.O ZENTYAL.

Instalación y configuración del Sistema Operativo Zentyal Server 5.0

Procedemos a la descarga de la imagen. Iso de la distribución Zentyal Server 6.0, mediante el siguiente link <http://www.zentyal.org/server/>.

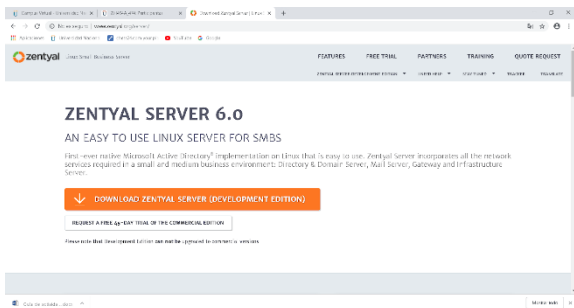


Fig 1. Descarga Zentyal

Una vez ya tengamos nuestra imagen ISO, damos comienzo a la instalación creando una nueva máquina virtual en nuestra herramienta Virtual Box, realizando las configuraciones pertinentes para tener un buen soporte de funcionamiento de nuestro nuevo sistema operativo.

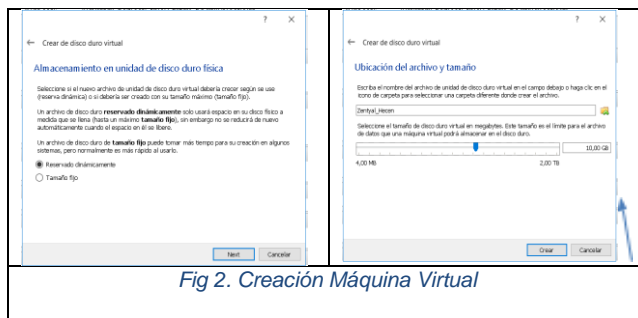


Fig 2. Creación Máquina Virtual

Configuración de Red

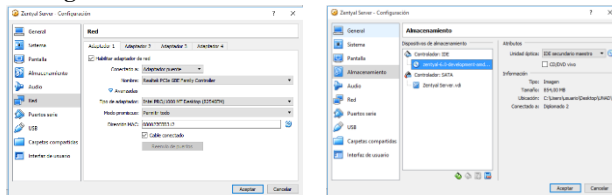


Fig 3. Configuración tarjetas de red

En este caso debemos de dejar las dos tarjetas como adaptador puente y modo promiscuo. (Wiki, 2017)

Ahora iniciamos la instalación de la distribución Linux Zentyal. Hacemos selección de nuestro idioma (Español).

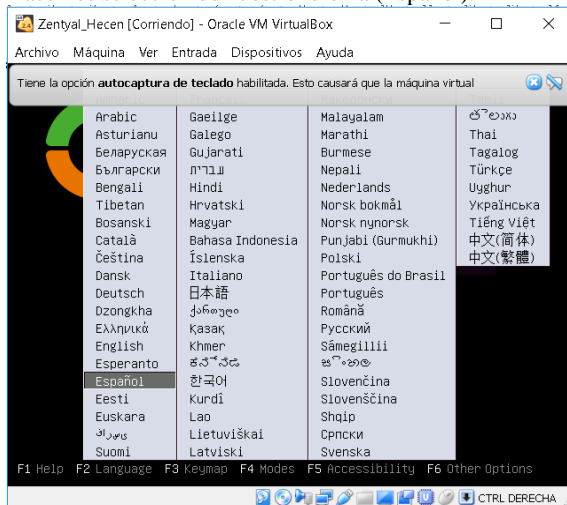
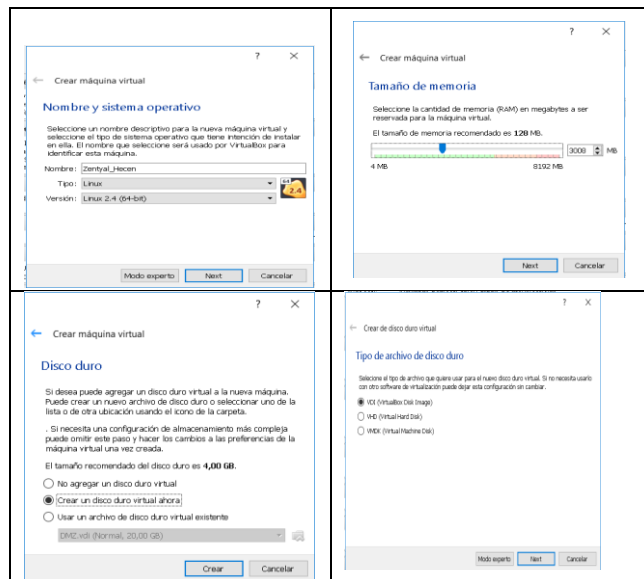


Fig 4. Configuración Idioma de Instalación

Instalación, para este proceso seleccionaremos la primera opción Instalar Zentyal 6.0-development (borrar todo el disco).



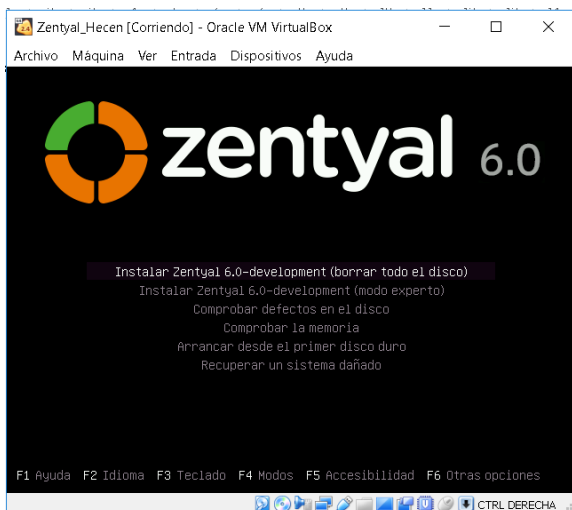


Fig 4.1. Instalación Zentyal

En el siguiente cuadro seleccionaremos nuestro país, para que el programa de instalación realice las respectivas configuraciones de zona horaria, localización del sistema.

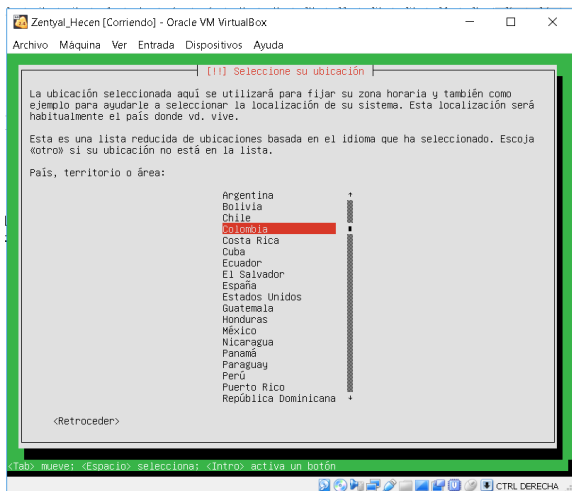


Fig 4.2. Instalación Zentyal

Realizamos la selección nuevamente de nuestro idioma, para la configuración de la distribución de nuestro teclado.

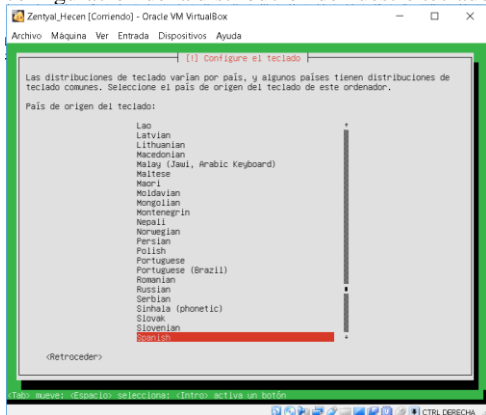


Fig 4.3 Instalación Zentyal

El asistente inicia con la carga de los componentes adicionales.

Esperamos unos pocos minutos a que realice la operación.

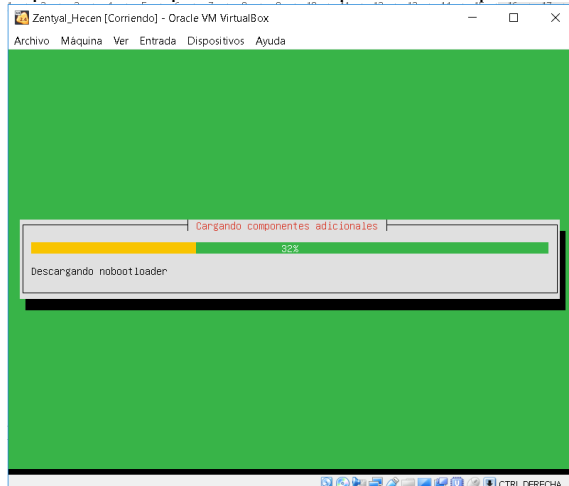


Fig 4.4 Instalación Zentyal

Luego debemos configurar la interfaz de red primaria o la interfaz de red interna, que en este caso usaremos la opción eth1. La interfaz de red eth0 la vamos a utilizar para la configuración del proveedor de servicios de internet IPS

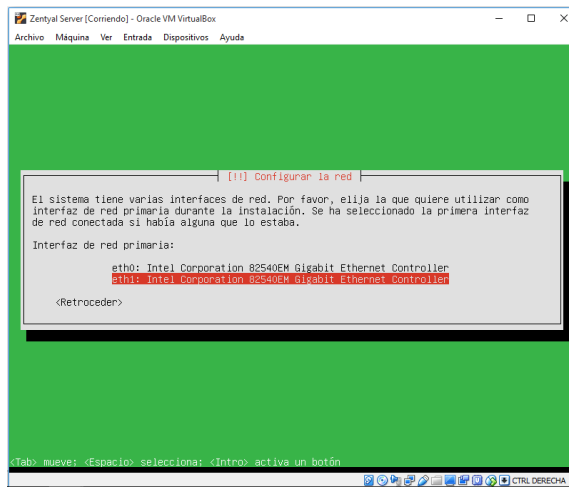


Fig 4.5 Instalación Zentyal

Esperamos a que el programa de instalación realice la configuración automática de la red con DHCP.

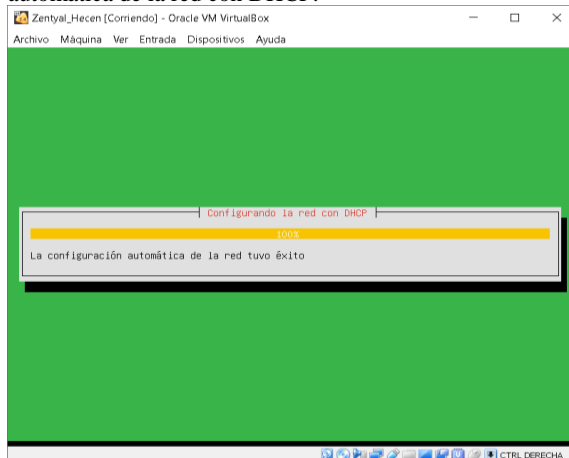
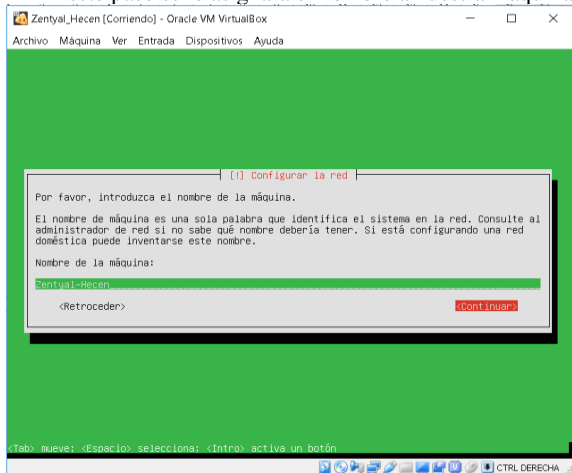
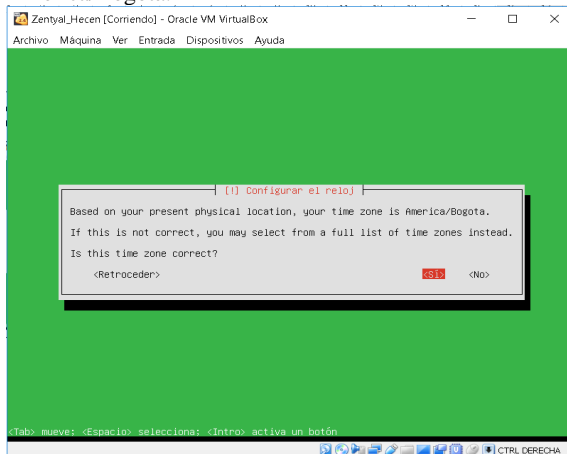


Fig 4.6 Instalación Zentyal

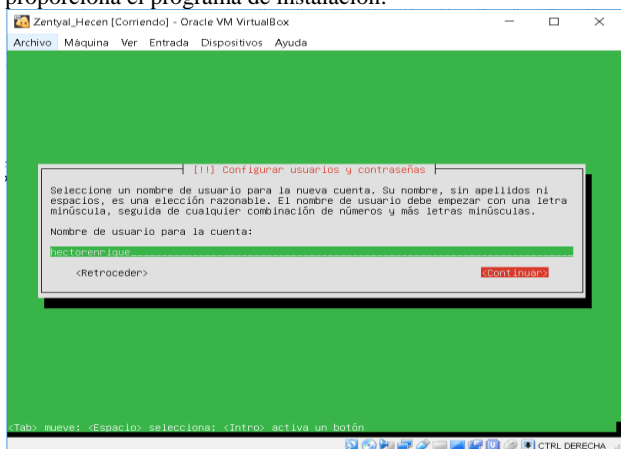
En este paso se le asignara el nombre a nuestra máquina.



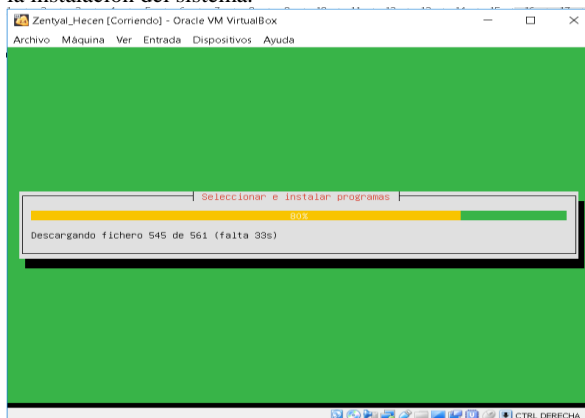
Luego confirmamos la zona horaria que nos indica que es América/Bogotá.



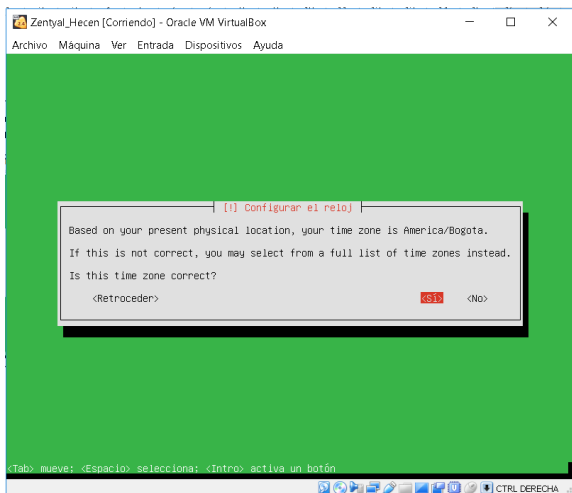
En el siguiente cuadro digitaremos el nombre para la nueva cuenta, teniendo en cuenta las recomendaciones que nos proporciona el programa de instalación.



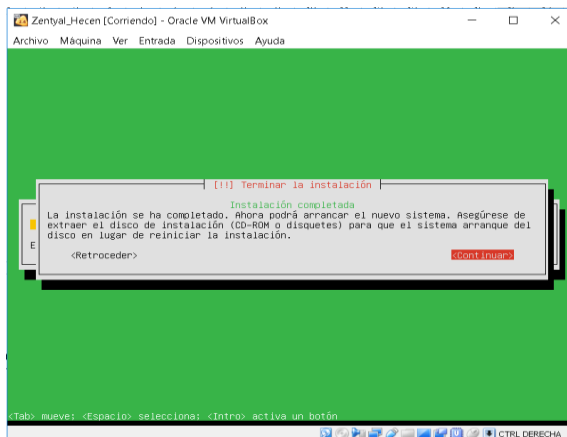
Después de que el programa de instalación realiza las procede a la instalación del sistema.



Establecemos la contraseña para nuestro nuevo usuario. Luego realizamos la introducción de la contraseña escogido nuevamente para que el programa de instalación realice la verificación correspondiente.



Automáticamente el programa de instalación realiza valga la redundancia la instalación de los programas predeterminados.



Luego de reiniciar la maquina se inicia el Zentyal e inicia el proceso de instalación de paquetes de Core. Debemos esperar hasta que finalice.

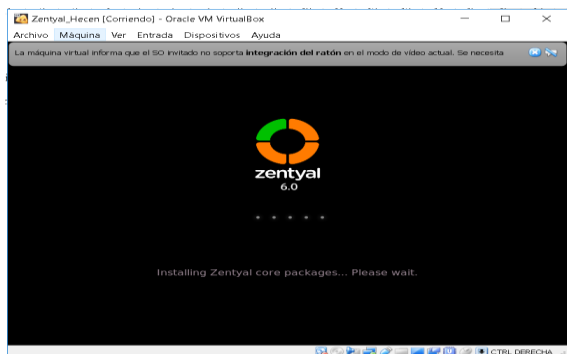


Fig 4.13 Instalación Zentyal

A – Configuración Inicial Zentyal



Fig 5 Configuración Zentyal

Procedimiento de configuración inicial en Zentyal



Fig 5 Configuración Zentyal

Muestra los modulo iniciales que se pueden agregar en la instalación. Es muy importante tener en cuenta que el proceso de instalación en este punto debe de estar de acuerdo con configuración que se va implementar en el servidor, puesto que al instalar módulos que no se van a utilizar puede acaparar recursos que un futuro nos pueden servir para otras funciones. Para esta primera etapa vamos a instalar los módulos de controlador de dominio, Network Configuration, servidor DNS, DHCP, NTP, y Firewall

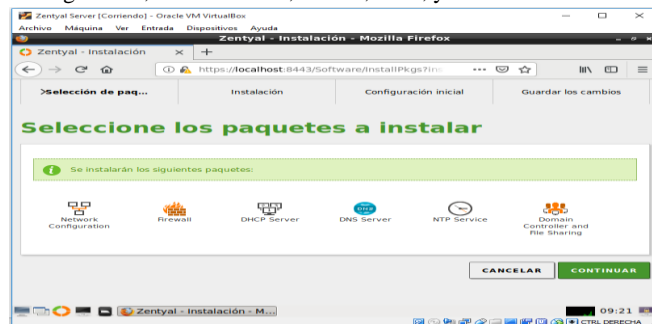


Fig 5.1 Configuración Zentyal

Una vez instalados los módulos continuamos con el proceso de configuración de los adaptadores de red. En este punto se debe de tener en cuenta que el adaptador de red principal eth1 (que es el mismo de la red interna), debe de estar en una segmentación diferente que la interfaz eth0 en donde va estar conectado el proveedor de servicios de internet IPS. Por eso dentro de la configuración vamos a estipular una conexión tipo DHCP para la red externa eth0 (el cual le asignara una dirección ip a nuestra tarjeta dentro del rango 192.168.0.x desde el router de internet) y vamos a colocar una dirección ip estática para nuestra red interna eth0 en una segmentación ip diferente (en este caso la 192.168.1.10), (UnderPro., 2014):

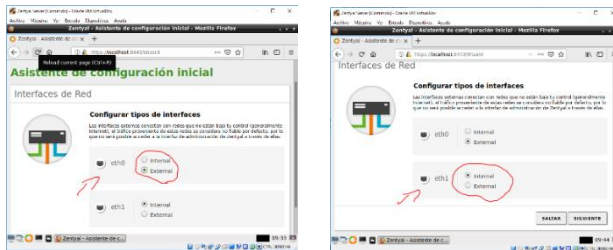


Fig 5.2 Configuración Zentyal

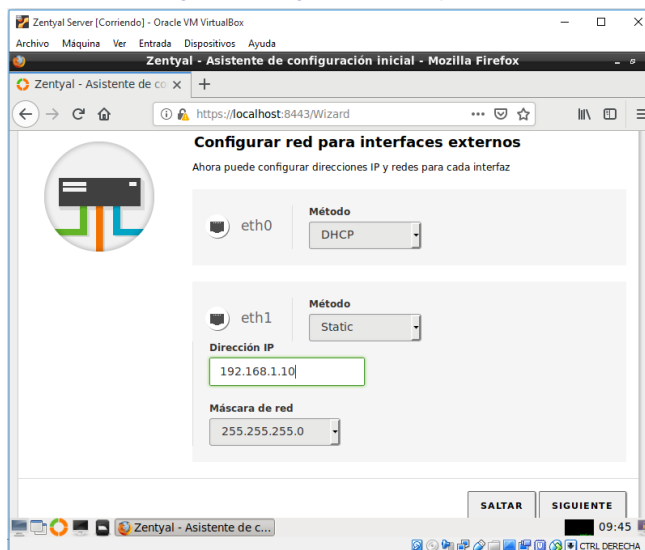


Fig 5.3 Configuración Zentyal

Después de configurar las tarjetas de red nos pregunta qué tipo de servidor vamos a configurar, en este caso vamos a configurar un servidor stand-alone y vamos a especificar un nombre de dominio para el servidor. (Para esta primera etapa de la configuración se va llamar “diplomadoandres.com”):

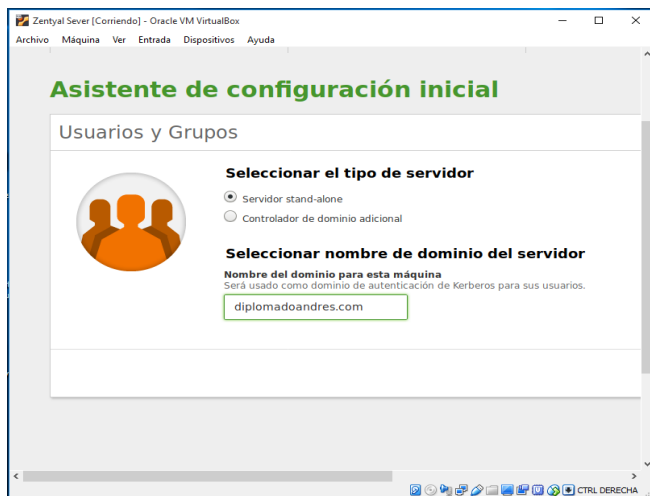


Fig 5.4 Configuración Zentyal

Una vez realizada la configuración inicial, continuamos con el desarrollo de las actividades propuestas.

V DESARROLLO DE LAS TEMÁTICAS

A- Temática 1: DHCP Server, DNS Server y Controlador de Dominio

Iniciamos esta primera etapa de la configuración del servidor Zentyal instalando el servidor DHCP. Lo primero que hacemos es verificar el estado de los módulos:



Fig 6 Activación modulo DHCP

Habilitamos el servicio guardando los cambios. Luego verificamos el estado de las tarjetas de red externa:



Fig 6.1 Configuración tarjeta de red Wan

e interna:



Fig 6.2 Configuración tarjeta de red Lan

Aclarando la segmentación de red estipulada previamente en la configuración inicial. Luego nos vamos al módulo de DHCP a la opción de configuración:



Fig 6.3 Configuración DHCP

Como podemos ver nos aparece un mensaje en donde no hay una dirección y rangos configurados, por lo que nos vamos a la opción de configuración en donde aparece nuestra red interna eth1.

Entrando en la configuración DHCP de nuestra tarjeta de red interna eth1 nos pide una serie de datos. Primero le especificamos la puerta de enlace en donde necesitamos que esta se encuentre dentro de la misma segmentación de red de la tarjeta, por ese en este caso su puerta de enlace es 192.168.1.1.

Continuamos con la selección del dominio que en este caso fue que configuramos previamente "diplomadoandres.com" y con el servidor DNS que el Zentyal configuro por default.

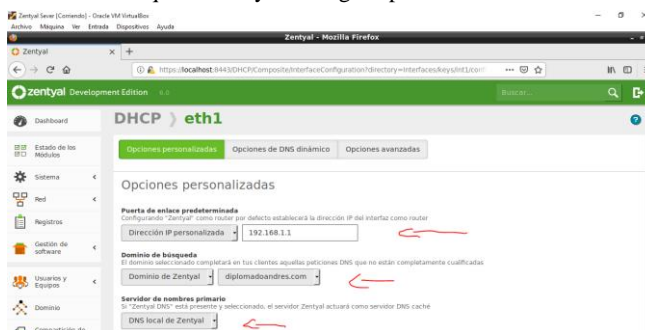


Fig 6.4 Configuración DHCP

Luego nos solicita que asignemos un rango de direccionamiento. En este caso voy a especificar que el servidor debe de asignarme ips de la 192.168.1.20 a la 192.168.1.100:

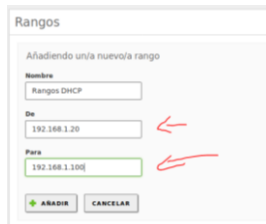


Fig 6.5 Asignación rango DHCP

Guardamos la configuración e iniciamos una maquina cliente Ubuntu para comprobar la configuración. Una vez inicie la maquina verificamos la Dashboard del servidor y corroboramos el funcionamiento:

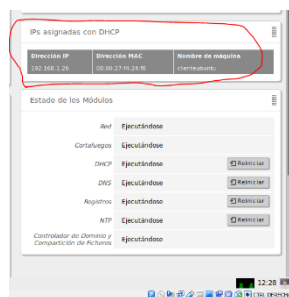


Fig. 6.6 Asignación IP Cliente

Como podemos ver el equipo cliente se conecta satisfactoriamente con la ip 192.168.1.26 que le asigna el servidor DHCP de Zentyal. Ahora realizaremos un ping en cada máquina para probar conexiones:

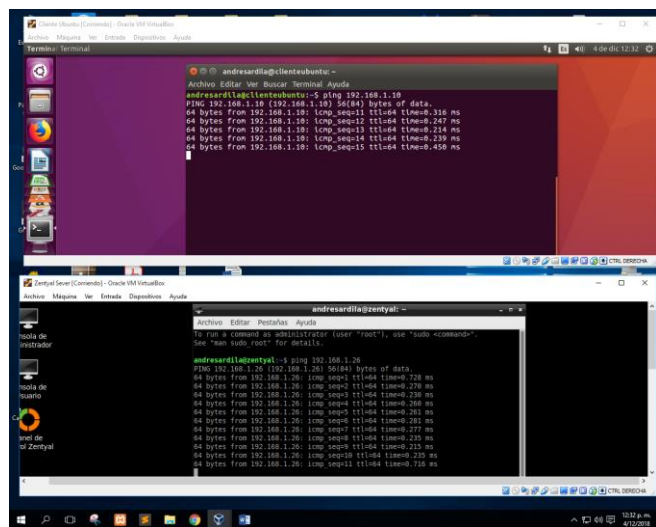


Fig 6.7 Demostración DHCP

Y de esta forma configuramos nuestro servidor DCHP. Ahora continuamos con la configuración del servidor DNS

Configuración Servidor DNS

Para configurar nuestro servidor de administrador de espacio de nombres de dominio (DNS) nos dirigimos a la opción de estado de módulos para verificar si nuestro servicio se encuentra instalado:



Fig 7 Activación Modulo DNS

Podemos ver que nuestro servidor DNS ya se encuentra instalado y habilitado. Ahora lo que tenemos que hacer es entrar a la opción DNS para poder verificar su configuración:

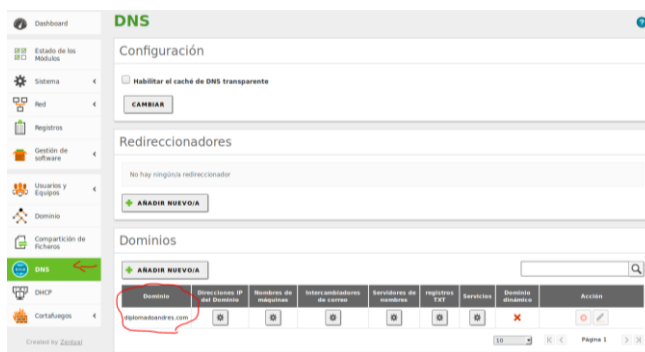


Fig 7.1 Configuración DNS

Nos encontramos el nombre de dominio que ya habíamos configurado previamente, ahora lo que tenemos que hacer es verificar que todas sus configuraciones son las adecuadas para que este servicio funcione adecuadamente. Empezamos con las direcciones ip del dominio:



Fig 7.2 IP de Dominio

Encontramos que nuestro dominio “diplomadoandres.com” está asociado a la dirección ip 192.168.1.10, que es la de nuestro servidor Zentyal. Continuamos con los nombres de maquina:



Fig 7.3 Nombre equipo Zentyal

Logrando identificar cada una de la configuración de nuestro servidor DNS ahora vamos a corroborar su funcionamiento. Lo primero que hacemos es verificar dentro de la configuración DHCP cual fue la configuración DNS:



Fig 7.4 Servidor de Nombre primario

Como podemos ver encontramos que el servidor de nombres primario está configurado el servidor DNS local de Zentyal y el dominio preconfigurado “diplomadoandres.com”, por lo que el mismo direccionamiento DHCP asignara esta configuración de dominio y DNS a nuestros equipos clientes. Ahora lo que vamos hacer es verificar que el servidor DNS está funcionando en nuestro equipo cliente. Lo primero que hacemos es ejecutar el siguiente

código par que nos de la configuración DNS que tienen en este momento el equipo cliente:

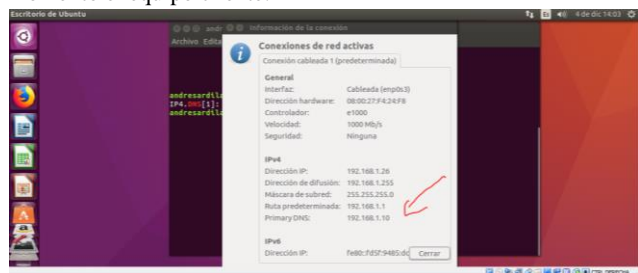


Fig 7.5 Demostración DNS en equipo Cliente

Podemos ver que el DNS primario del equipo cliente es 192.168.1.10 que es la misma configurada dentro del servidor DNS de nuestro servidor. Como configuramos previamente el adaptador de red eth0 para administrar nuestra entrada a internet ahora tenemos que verificar si el internet que llega por esa interfaz está administrada por el servidor DNS al equipo cliente. Para esto vamos a entrar a internet en ambas máquinas:

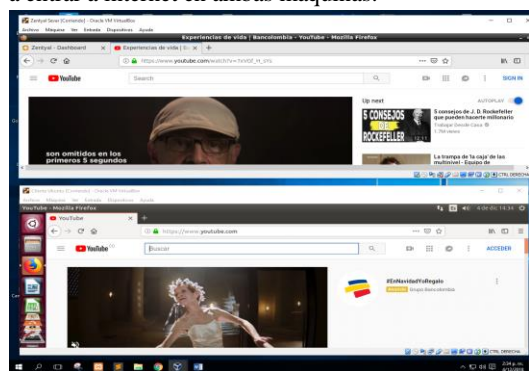


Fig 7.6 Navegación Equipo Cliente

Y a realizar un ping a google:

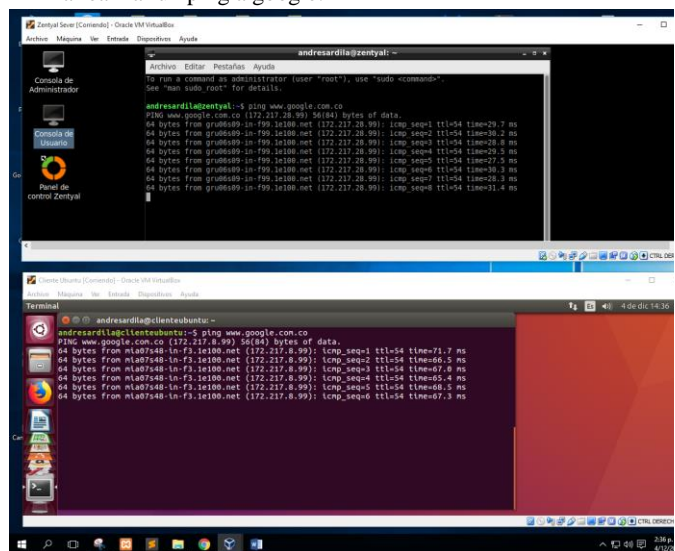


Fig 7.7 Demostración Ping

De esta forma configuramos nuestro servidor DNS.

Configuración de controlador de dominio

Esta configuración tiene el objeto de vincular el servidor con los equipos clientes para gestionar la administración de servicios por medio de una autenticación que garantiza la seguridad administrativa del mismo. El controlador de dominio se manifiesta desde el servidor desde un IP que es la identificación en red del mismo y esta se traduce a una palabra (como domini.com) el cual es el nombre que identifica dicha dirección de red.

Este proceso permitirá que los computadores conectados al servidor estarán sujetos a una serie de configuraciones y servicios específicos (servicios dns, firewall, dhcp, archivos compartidos, conexiones vpn entre otros) que van a garantizar su seguridad y funcionamiento en la red.

Para configurar el controlador de dominio desde el servidor Zentyal lo primero que debemos hacer (teniendo en cuenta de haber realizado satisfactoriamente las configuraciones pasadas de dhcp y dns) es entrar al panel administrativo e instalar o verificar que estén instalados los paquetes de controlador de dominio:



Fig 8 Activación Modulo LDAP

Como podemos ver encontramos que el servicio de controlador de dominio ya se encuentra instalado. Si no está instalado nos vamos a opción “Gestor de software” y lo instalamos. Luego de instalarlo tenemos que ir la opción de “Dominio” la cual nos va permitir configurar nuestro dominio:

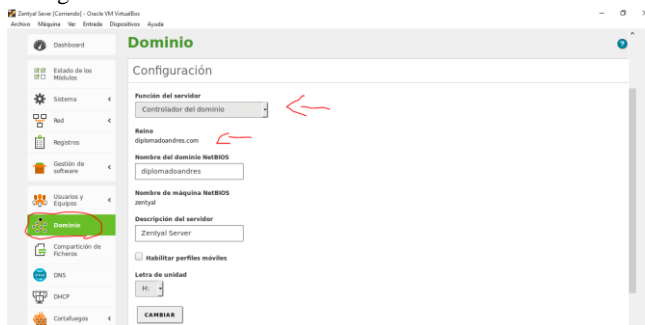


Fig 8.1 Configuración Dominio

Como podemos ver encontramos la opción de función del servidor que en este caso es el controlador de dominio (que previamente instalamos en la configuración inicial de Zentyal). En esta opción podemos configurar un dominio adicional si así lo deseamos. Luego encontramos el nombre de del “Reino” o el nombre de dominio que va traducir en una palabra la dirección IP del controlador del dominio que en este caso es la misma del servidor Zentyal. Por ultimo encontramos el nombre del servidor que en este caso es “Zentyal”. Una vez que verifiquemos que nuestro

dominio “diplomadoandres.com” este configurado vamos a verificar sus datos desde consola:

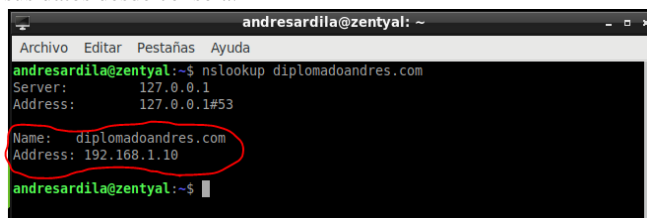


Fig 8.2 Validación DNS Dominio

Podemos ver que el dominio configurado está respondiendo directamente a la IP configurada en el servidor Zentyal 192.168.1.10. Ahora vamos a configurar nuestro controlador de dominio. Lo primero que hacemos es entrar en la opción de controlador de dominio llamado “Usuarios y Equipos” desde el servidor:

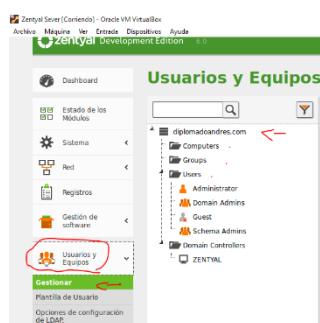


Fig 8.2 Usuario y Equipos AD

En este punto podemos ver nuestro controlador de dominio “diplomadoandres.com” con las subcarpetas “Computadores”, “Grupos”, “Usuarios” y “Controlador de Dominio”.

Ahora para continuar con la configuración vamos a crear primero un usuario administrador del controlador de dominio, el cual va tener el privilegio de autorizar a los equipos clientes conectarse.

En este caso mi usuario se llama “admindominio” y va ser nuestro usuario administrador de dominio, por eso es importante agregarlo al grupo “Domain Admins”. Luego de crear nuestro usuario administrador vamos a crear un grupo para administrar los usuarios Ubuntu.



En este caso el grupo se va llamar “ubuntu”.

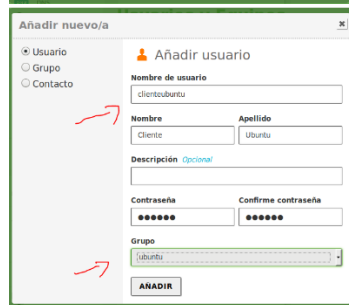


Fig 8.3 Creación de Usuario y grupo de Dominio

Una vez creado nuestro grupo vamos a crear un usuario nuevo para que el equipo Ubuntu pueda conectarse al controlador de dominio. En este caso se va llamar “clienteubuntu”

Ahora vamos a agregar nuestro equipo Ubuntu a nuestro dominio. Iniciamos nuestra máquina virtual y verificamos nuevamente que el servidor dhcp le asigne su respectiva ip:

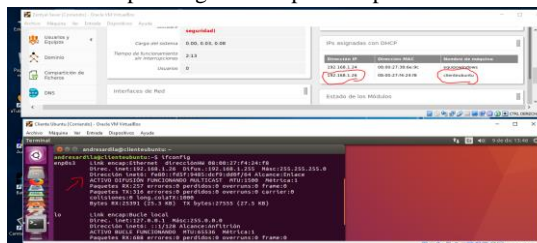


Fig 8.4 Direccionamiento IP equipo Cliente

Como podemos ver asigno la ip 192.168.1.26 que es la misma cuando realizamos la prueba con este equipo Ubuntu. Ahora miramos si la configuración del dominio en el equipo cliente es la adecuada:

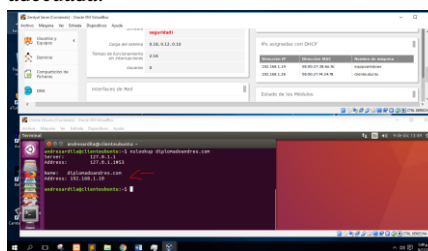


Fig 8.5 Confirmación DNS Zentyal desde Cliente

Como podemos ver efectivamente el nombre de dominio está respondiendo a la dirección ip del servidor que es 192.168.1.10. Una vez realizada esta prueba nos disponemos a configurar el equipo cliente para unirlo a nuestro controlador de dominio. Para esto descargamos el programa PowerBroker de la página oficial:

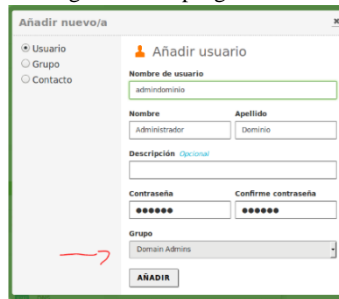


Fig 8.6 Creación usuario administrador del dominio

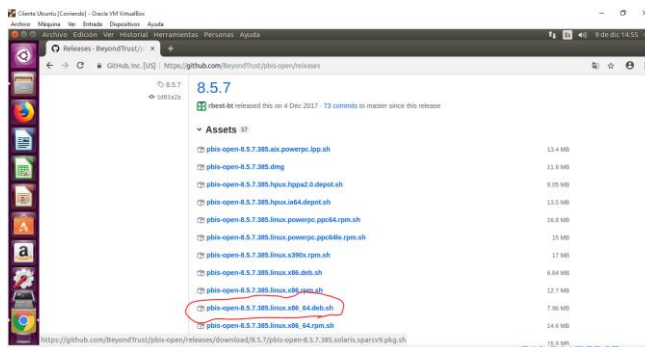


Fig 8.7 Descarga script pbis

Le damos permisos al archivo descargado y lo ejecutamos de la siguiente forma:

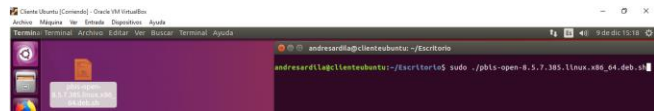


Fig 8.8 Instalación de pbis

Después de reiniciar el equipo adjuntamos la configuración del servidor dns y nombre de dominio a la interfaz de red:

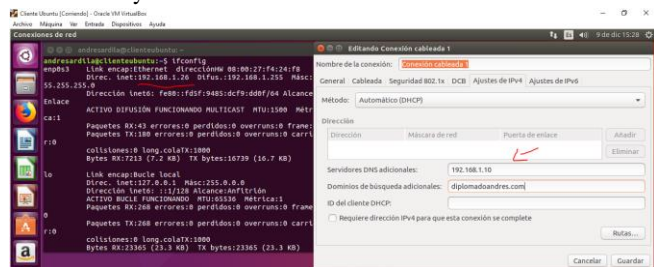


Fig 8.9 Ingresos DNS servidor a cliente Ubuntu

Entramos en la carpeta /opt/pbis/bin y ejecutamos el siguiente código:



Fig 8.10 Ingreso al Domino Zentyal

Gestionamos credenciales y de esta forma unimos nuestro equipo cliente al controlador de dominio (KnowITFree, 2016)

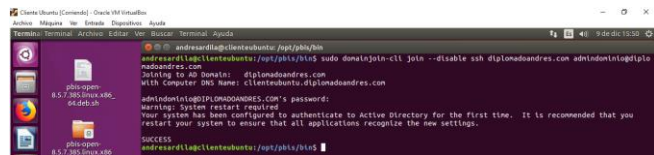


Fig 8.11 Ingreso al Domino Zentyal

Revisamos la configuración desde el servidor:

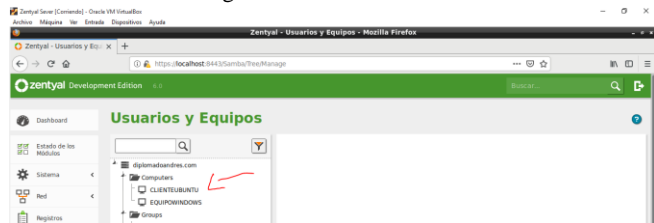


Fig 8.12 Cliente Ubuntu en contenedor computers

Como podemos ver el equipo ya está agregado. Ahora tenemos que configurar el panel de ingreso a la cuenta del controlador desde el equipo porque esta no la asocia automáticamente. Empezamos entrando nuevamente al usuario local y entramos al terminal para editar el siguiente archivo y agregamos la siguiente línea de código:

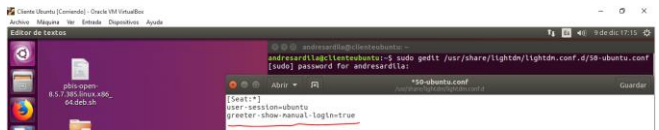


Fig 8.13 Habilitar acceder a usuarios del Dominio

Y después de reiniciar podemos ver que tenemos la opción de ingresar a nuestro servidor con la cuenta creada previamente (**Open, 2018**):

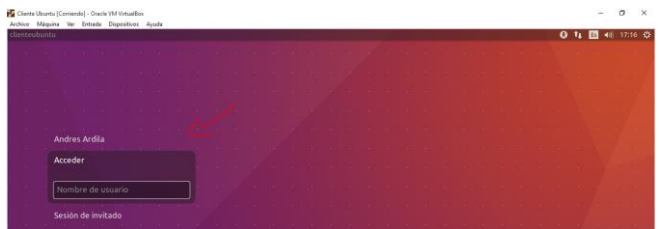


Fig 8.14 Inicio de sesión usuario de Dominio

Ingresamos con las credenciales del usuario creadas en el controlador de dominio del servidor y una vez ingresamos realizamos una prueba de identificación de controlador de dominio:

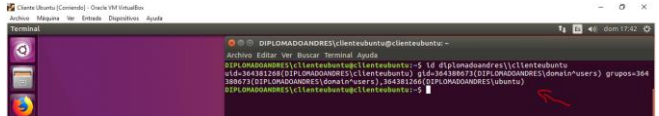


Fig 8.15 Prueba de identificación de Dominio

Como podemos ver nuestro equipo cliente ya se encuentra unido a nuestro controlador de dominio gestionado desde el servidor Zentyal.

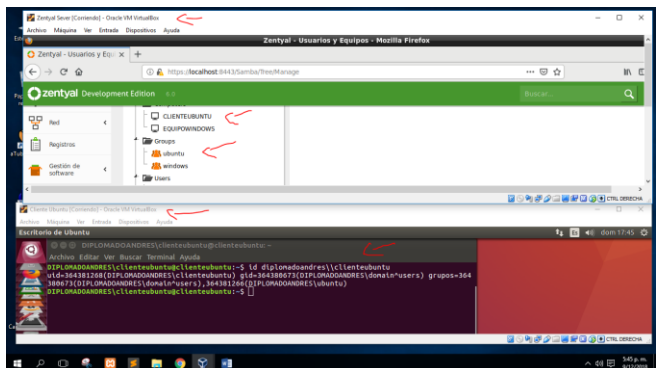


Fig 8.16 Prueba de identificación de Dominio

Desarrollo de la Temática

B- Temática 2: Proxy no transparente

Esta temática fue desarrollada por el Estudiante Luis Fernando Umbarila.

Se inicia por la instalación y activación del modulo HTTP Proxy

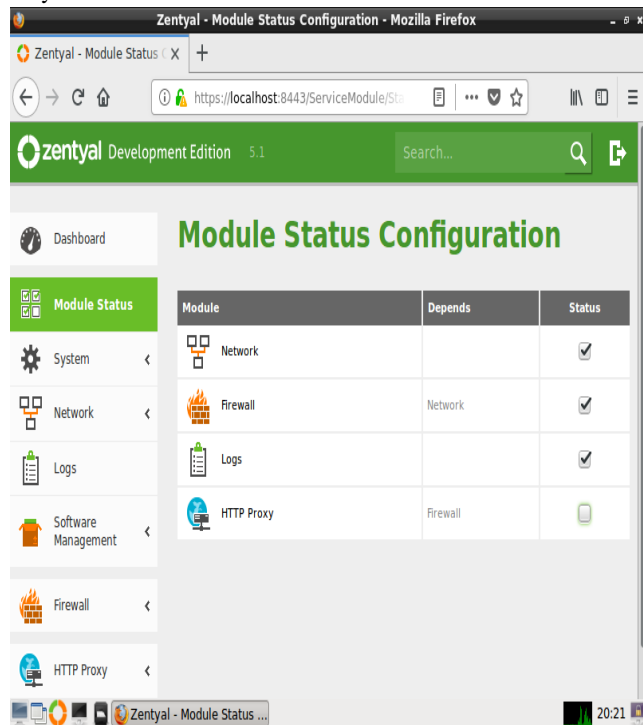


Fig 9 Activación Proxy

Se acepta la configuración

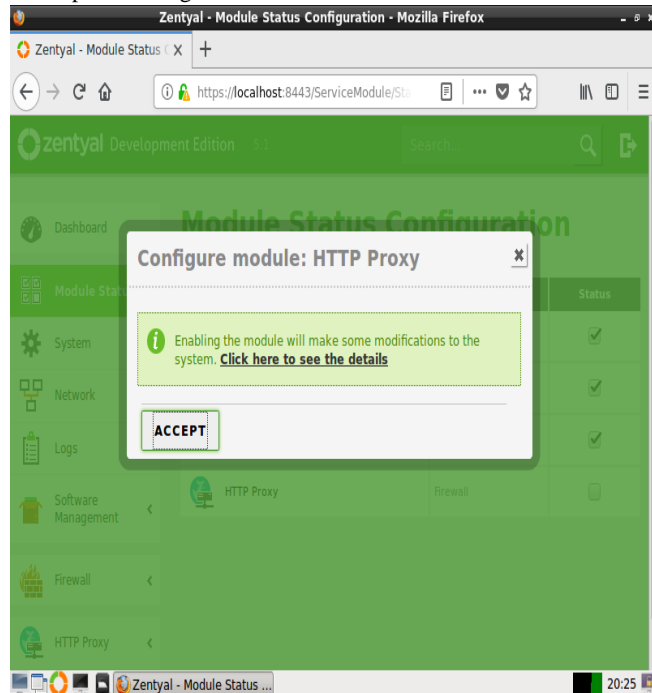


Fig 9.1 Activación Proxy

Se modifica la interfase eth1 por WAN

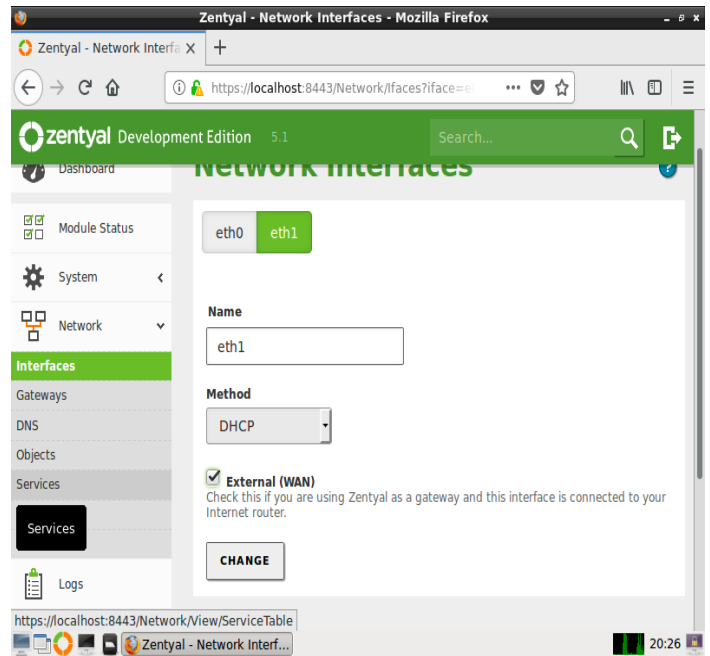


Fig 9.2 Configuración tarjeta de red Proxy

Se muestra el progreso

Se están guardando los cambios

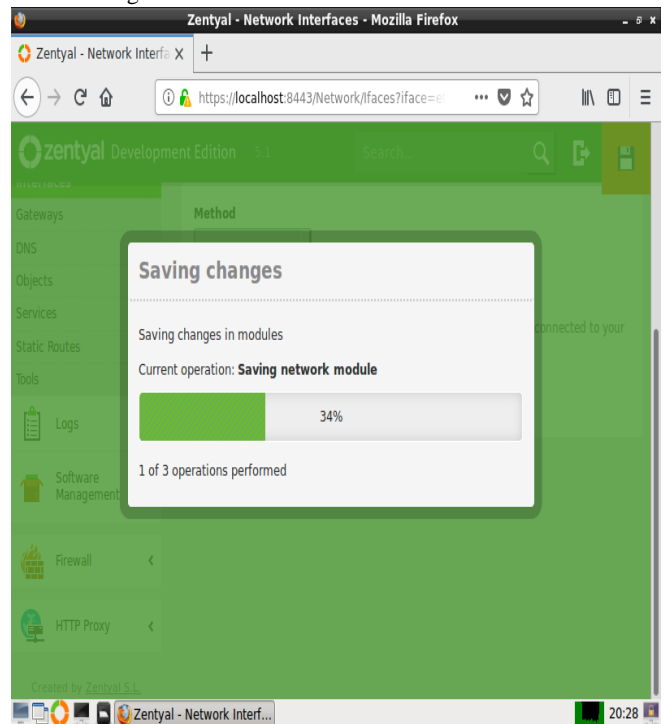


Fig 9.4 Guardando cambios

Se muestran los cambios guardados

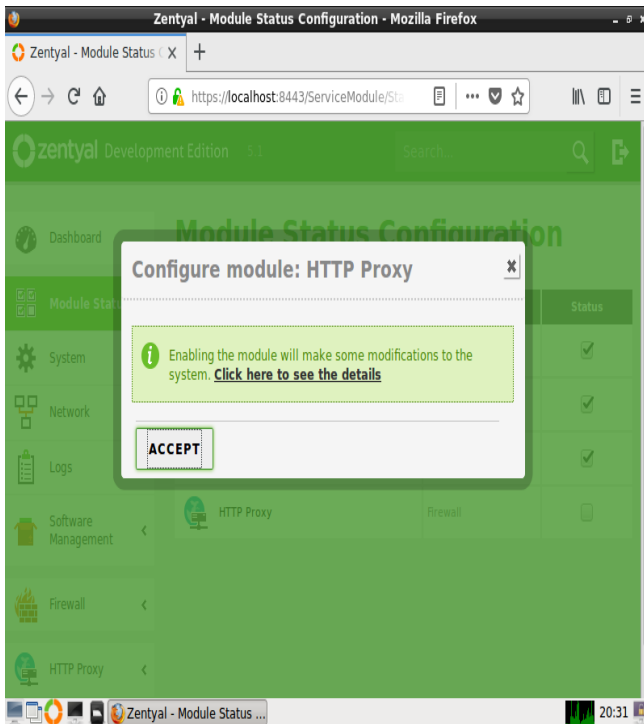


Fig 9.5 proxy habilitado

Se confirma cambios

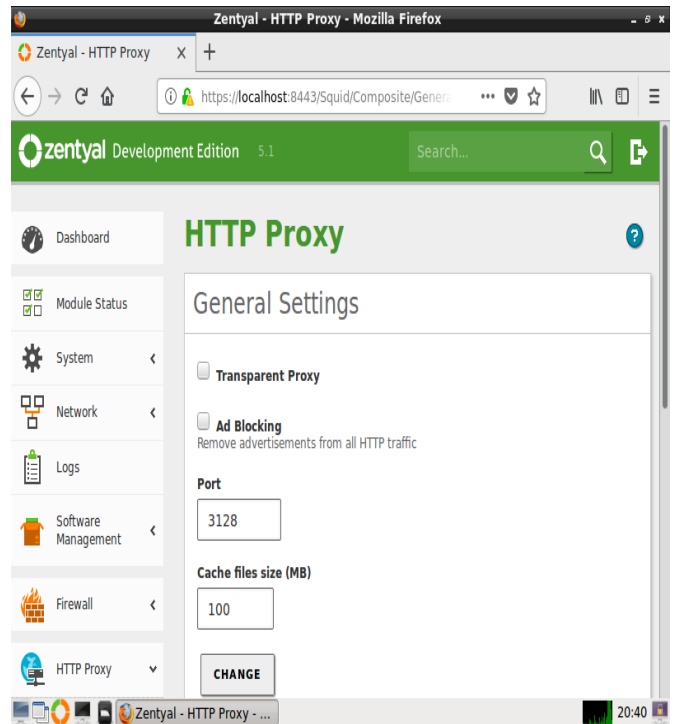


Fig 9.7 Configuración puerto servidor proxy

Se guardan los cambios

Se cambia el proxy

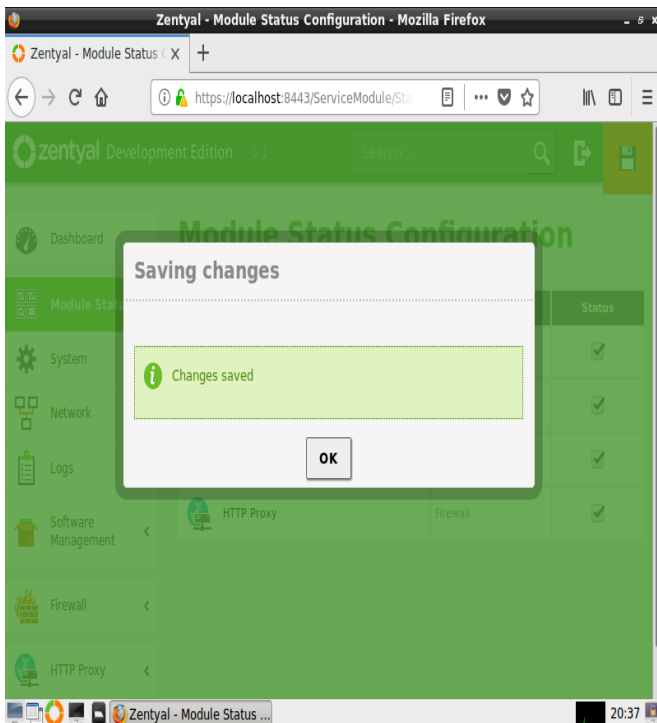


Fig 9.6 cambios aplicados

Se configura el proxy con el puerto 3128

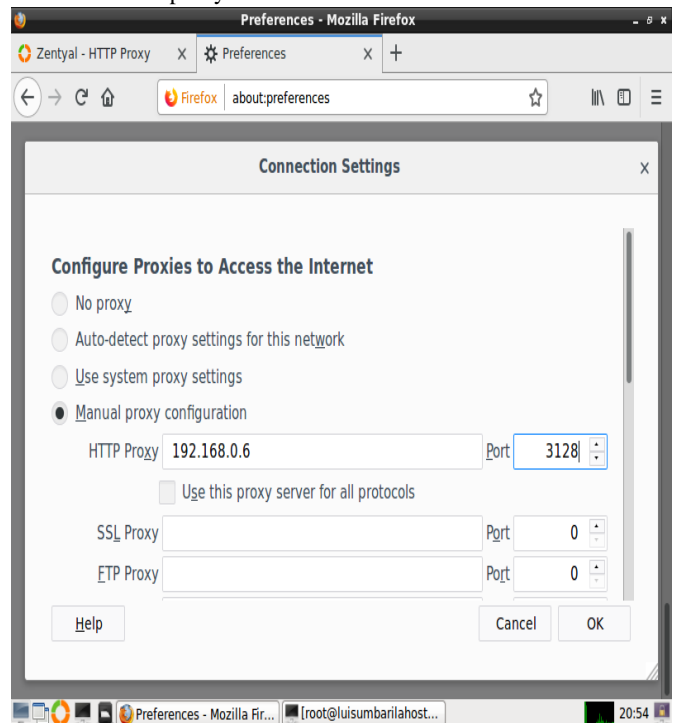


Fig 9.8 Configuración dirección proxy

Se ejecuta una prueba con resultado exitoso

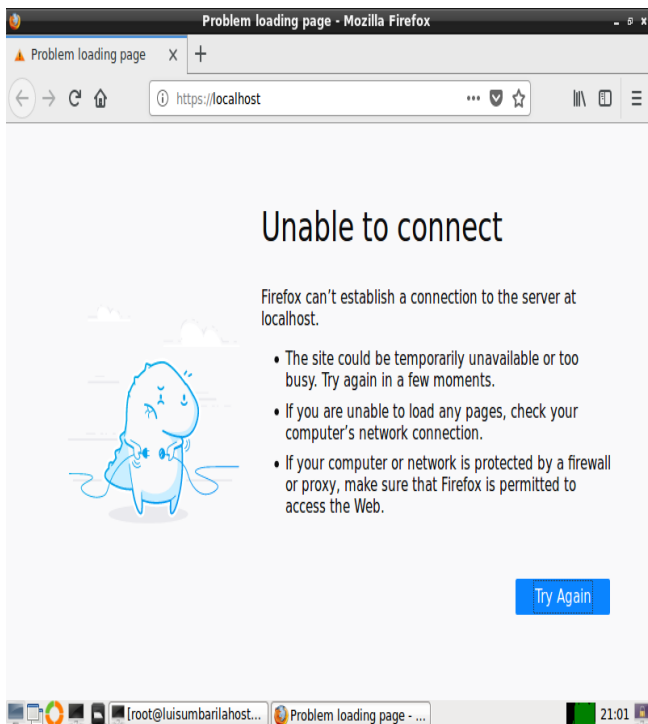


Fig 9.9 prueba servidor proxy

Se vuelve a cambiar el proxy y el resultado es exitoso

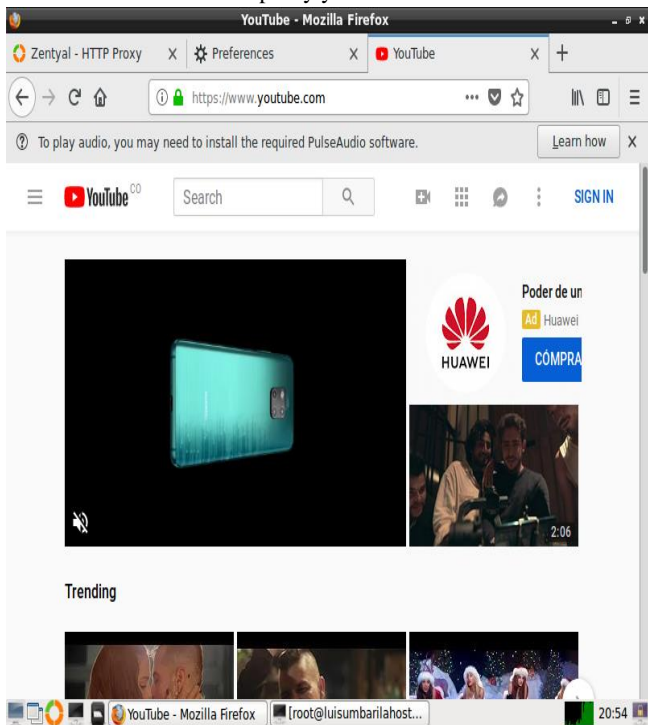


Fig 9.10 prueba de navegación exitosa servidor proxy

C- Temática 3: Cortafuegos
Morales Hernández

El siguiente paso será comprobar las configuraciones que hemos realizado. Para esto a continuación vamos a iniciar nuestra máquina virtual con Ubuntu desktop previamente instalada para comprobar la configuración de la red. Una vez iniciada la maquina verificamos con el comando *ifconfig* la IP

que obtuvo, 10.10.20.10 que está de acuerdo con las configuraciones realizadas con los rangos. (Lema, 2016)

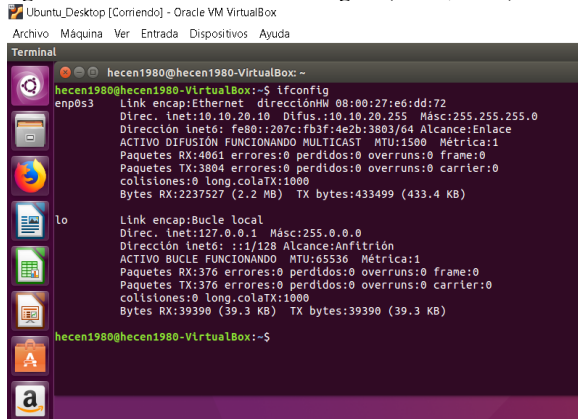


Fig 10 Configuración IP

Realizamos un ping a la IP del Zentyal para verificar que se pueden conectar.

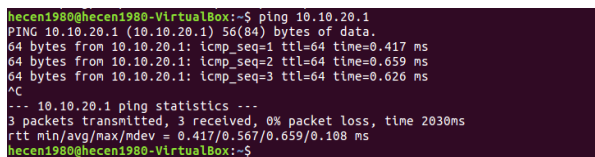


Fig 10.1 prueba de conexión con servidor Zentyal

Temática 3: Cortafuegos

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. (Alvarez, 2013)

Para el desarrollo de este paso, primero nos vamos a dirigir a la ruta **Cortafuegos-Filtrado de paquetes**, y una vez allí nos dirigimos cuadro con el título de **Reglas de filtrado para las redes internas**.

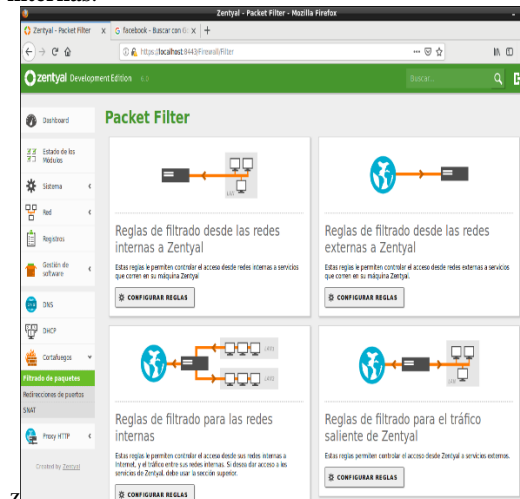


Fig 10.2 ingreso a reglas de filtrado

Ahora procedemos a añadir cada una de las reglas de filtrado para la restricción de la apertura de sitios o portales Web de entretenimiento y redes sociales.

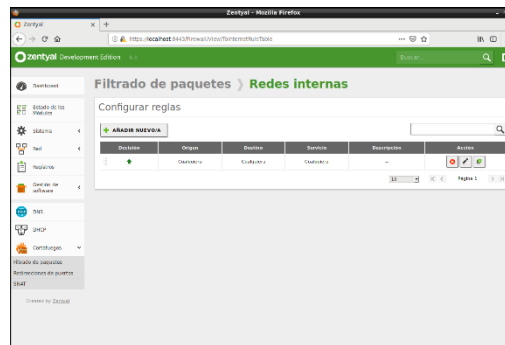
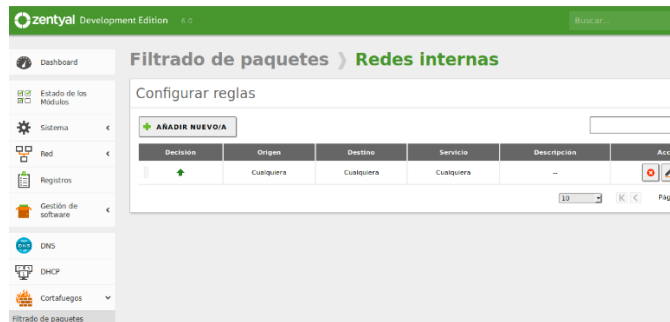


Fig 10.3 ingreso a reglas de filtrado

Restricción de la red social Facebook

Para este proceso nos dirigimos al servicio de **Cortafuegos** ubicado en el panel de la mano izquierda y damos clic, en el menú emergente seleccionamos la opción **Filtrado de paquetes**.

Antes del siguiente paso, evidenciamos que tenemos navegabilidad en el Ubuntu Desktop hacia la página, que con el cortafuegos de Zentyal queremos bloquear, comprobación que realizamos tanto en el navegador como también por medio de la consola digitando la siguiente línea de comando: `ping www.facebook.com`.

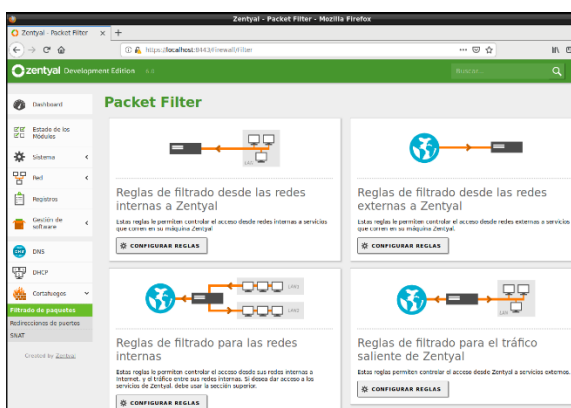


Fig 10.4 Prueba de navegación

Interfaz de usuario vamos al título **Reglas de filtrado para las redes internas** y damos clic el botón con el título **Configurar Reglas**.

Continuado con los pasos de bloqueo mediante el servicio de cortafuegos de Zentyal, en la nueva interfaz realizamos las siguientes configuraciones:

- ✓ En el menú desplegable debajo del título **Decisión**, seleccionamos en el menú **Denegar**.
- ✓ En el menú desplegable debajo del título **Origen**, seleccionamos en el menú **Cualquiera**.
- ✓ En el menú desplegable debajo del título **Destino**, seleccionamos en el menú **Ip Destino** y en la caja que aparece digitamos la dirección Ip de Facebook (la podemos obtener haciendo ping en el Ubuntu Desktop).

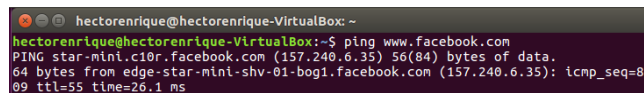
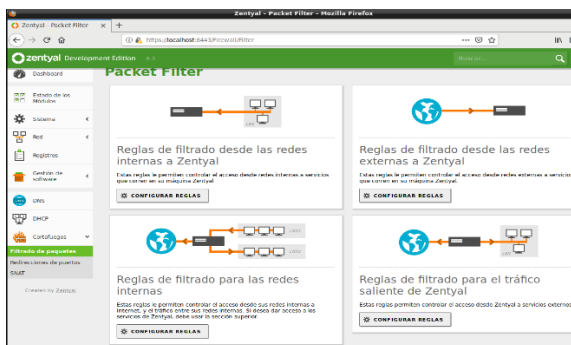


Fig 10.5 Prueba de navegación

- ✓ En el menú desplegable debajo del título **Servicio**, seleccionamos **Cualquiera**.

En el siguiente cuadro damos clic en el botón **Añadir Nueva**.

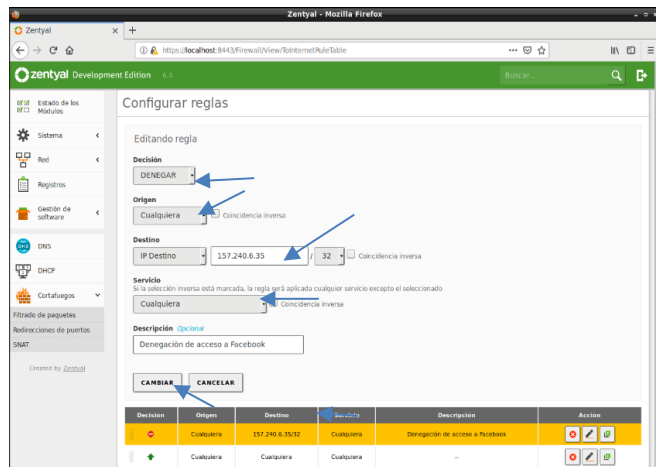


Fig 10.6 Nueva regla firewall

En el nuevo pantallazo evidenciamos que queda añadida la nueva regla en nuestro cortafuegos y le damos guardar.

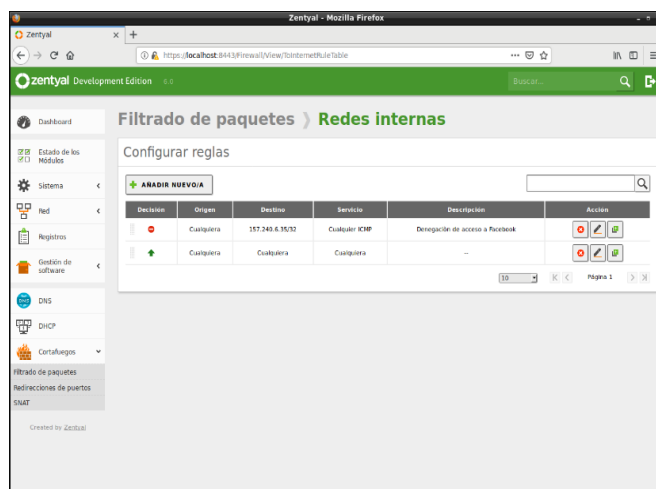


Fig 10.6 Nueva regla firewall

Ahora comprobamos que la regla ha sido configurada efectivamente. Nos dirigimos al Ubuntu Desktop, y comprobamos tanto en el navegador como también por medio de la consola, en ésta última con el comando **ping** www.facebook.com.

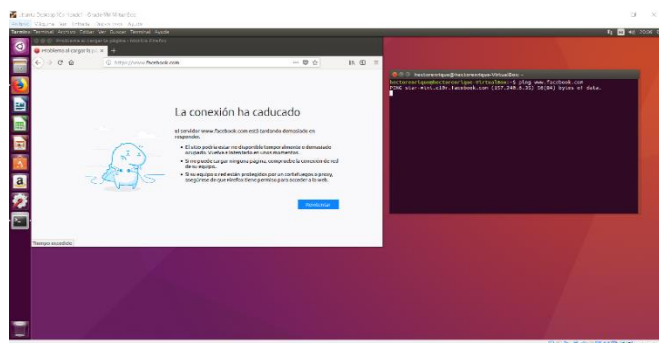


Fig 10.7 Bloqueo de navegación Facebook

Nota: para que la configuración tome efecto, debemos reiniciar nuestro navegador.

Y comprobamos que se tenga navegabilidad hacia otras páginas. Para mi ejemplo **youtube**.

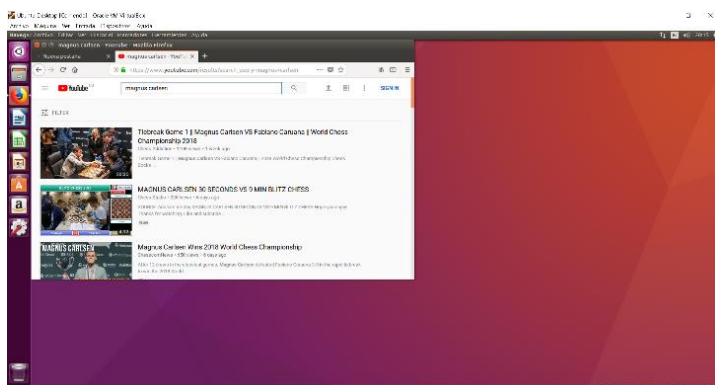


Fig 10.8 prueba de navegación youtube

D -Temática 4: File Server y Print Server

File server

Esta temática fue desarrollada por el Estudiante Iván Darío Restrepo

Debido a que File Server se debe montar sobre un LDAP, se procede con su instalación.

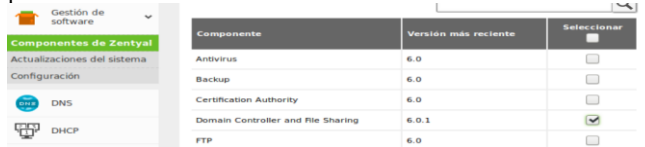


Fig 11 Activación modulo controlador de domino y file sharing

Se realiza activación del modulo



Fig 11.1 Guardado de modulo

En el menú Dominio creo un Domino bajo el cual estarán mis servicios.

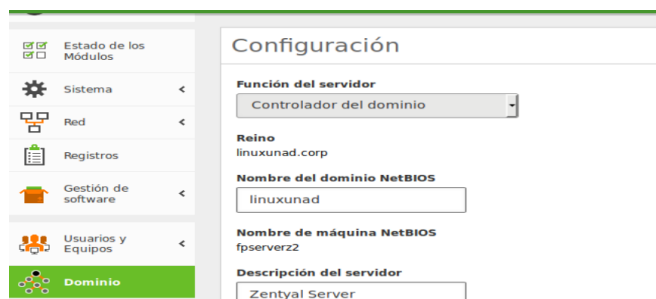


Fig 11.2 Configuración controlador de dominio.

Opciones de configuración de LDAP.



Fig 11.2 controlador de dominio.

En el menú Gestionar creo un usuario con el cual posteriormente realizare pruebas en una máquina del Dominio.

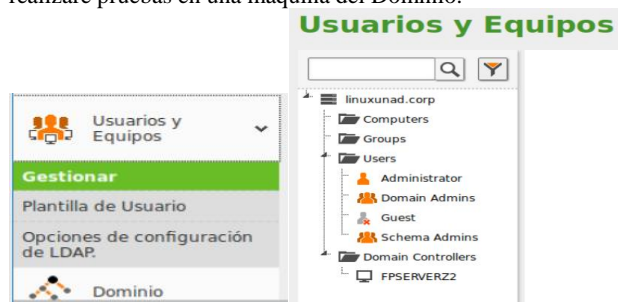


Fig 11.3 Modulo de usuarios y equipos.

Creo el usuario mramirez



Fig 11.4 Creación de usuario para pruebas

Lo añado a grupo de seguridad Documentación



Fig 11.5 Creación de grupo de Documentación

Obviare la parte en la parte en la que se suben los equipos cliente al Dominio puesto que ya se realizó en la temática 1. Realizo la instalación del File Server ingresando por el menú Compartición de Ficheros que se instalado con el servicio Domain Controller and File Sharing.



Fig 11.6 Ingreso a Compartición de Archivos

Se procede a añadir un nuevo fichero por la opción añadir nuevo. Añadir el primer recurso compartido en el cual se podra acceder desde los equipos del dominio con los usuarios del dominio al directorio que comparto. Cuando se escoge la ruta del compartido sea Directorio bajo Zentyal se guardará en /home/samba/share/company.



Fig 11.7 Creación de recurso compartido

Ahora se hace lo mismo, pero se compartirá un directorio con aplicaciones.



Fig 11.8 Creación de recurso compartido

Ya están creados los recursos compartidos



Fig 11.9 Ingreso a las ACL

Se ingresa a la opción control de acceso y se añade una nueva ACL “lista de control de acceso” y añado al usuario mramirez con permisos de lectura y escritura para que pueda utilizar el directorio DocumentosLinux.

Control de Acceso

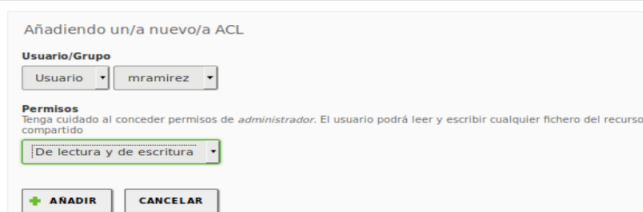


Fig 11.10 Permisos de usuario dentro de ACL

Ahora ingreso con el usuario mramirez a un equipo cliente Ubuntu

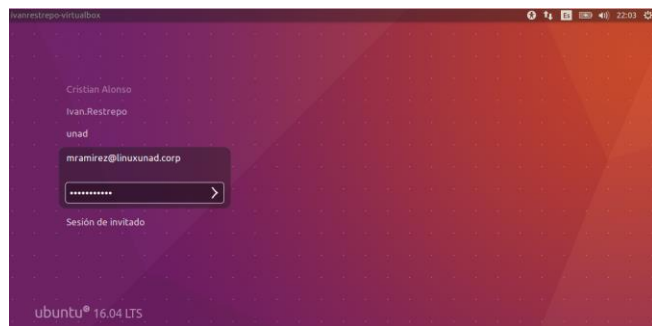


Fig 11.11 inicio de sesión usuario de prueba

Puedo visualizar por medio del entorno grafico que ya están los ficheros compartidos con el file server.

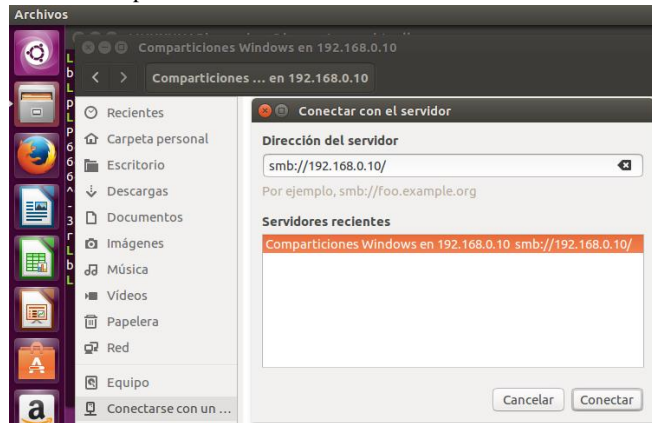


Fig 11.12 Ingreso a directorios compartidos

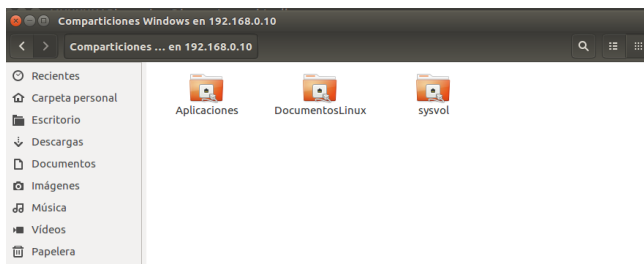


Fig 11.13 validación de directorios compartidos

Para montar el directorio compartido en Linux creo un directorio

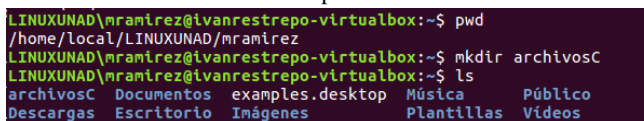


Fig 11.14 Directorio local para montar Directorio compartido

Monto el directorio compartido en el directorio creado.

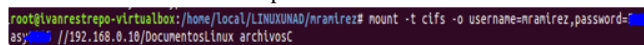


Fig 11.15 Montaje de directorio compartido

Creo un documento en la compartida

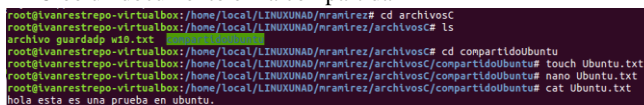


Fig 11.16 Creación de archivo compartido

Prueba Windows, ingreso con el usuario mramirez

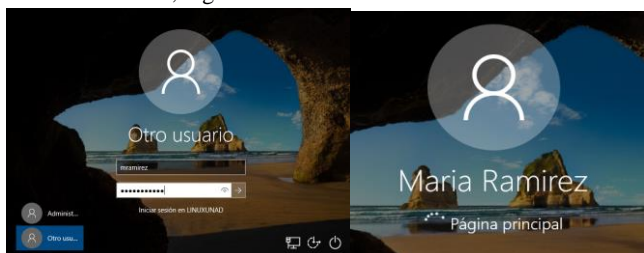


Fig 11.17 Inicio de usuario en equipo Windows

De puede visualizar el documento compartido desde UbuntuDesktop

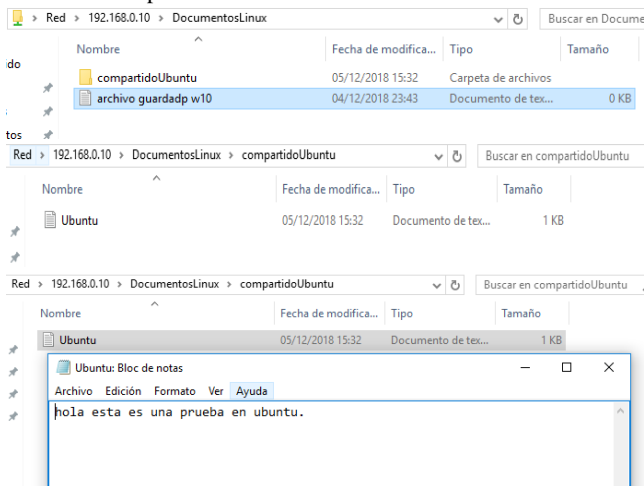


Fig 11.18 prueba de ingreso a archivo compartido

Finalmente se demuestra un file server funcional y multiplataforma.

Print Server

Como se puede evidenciar en Zentyal no se encuentra ningún módulo de instalación o para compartir impresoras desde su versión 5.0. Por tal razón investigando encontré una forma de hacerlo con CUPS (Common UNIX Printing System), (Chacón, s.f.) (Documentation, s.f.)

Instalación de CUPS

```
ivanrestrepo@fserver22:~$ sudo apt install cups
[sudo] password for ivanrestrepo:
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias
Leyendo la información de estado... Hecho
Se instalarán los siguientes paquetes adicionales:
bc cups-client cups-common cups-core-drivers cups-daemon cups-filters
cups-filters-core-drivers cups-ipp-utils cups-ppdc cups-server-common
ghostscript libcupsctl libcupsfilters1 libcupsmime1 libcupsppdc1
libfontembed1 libqpdf21 poppler-utils ssl-cert
Paquetes sugeridos:
cups-bsd foomatic-db-compressed-ppds | foomatic-db printer-driver-hpcups
hplip cups-pdf smbclient xpp printer-driver-gutenprint antiword docx2txt
ghostscript-x openssl-blacklist
Paquetes recomendados:
avahi-daemon colord printer-driver-gutenprint cups-browsed liblouisdml-bin
| liblouis-bin gfonts qpdf
Se instalarán los siguientes paquetes NUEVOS:
bc cups cups-client cups-common cups-core-drivers cups-daemon cups-filters
cups-filters-core-drivers cups-ipp-utils cups-ppdc cups-server-common
ghostscript libcupsctl libcupsfilters1 libcupsmime1 libcupsppdc1
libfontembed1 libqpdf21 poppler-utils ssl-cert
0 actualizados, 20 nuevos se instalarán, 0 para eliminar y 0 no actualizados.
```

Fig 12 Instalación de CUPS

Ya podemos empezar a configurar el servicio de impresión en Zentyal ingresando ya no por el puerto 8443 sino por el puerto 631. <https://localhost:631/admin>.

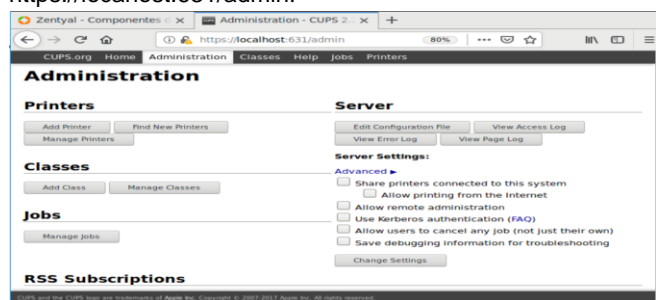


Fig 12.1 Administración CUPS

Se ingresa por add printer con usuario y contraseña

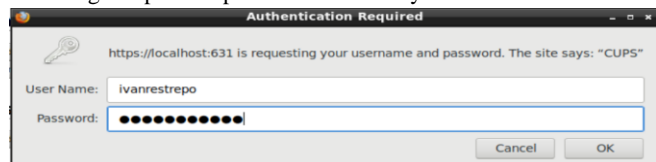


Fig 12.2 Ingreso de credenciales

Se agrega una impresora para pruebas

Add Printer

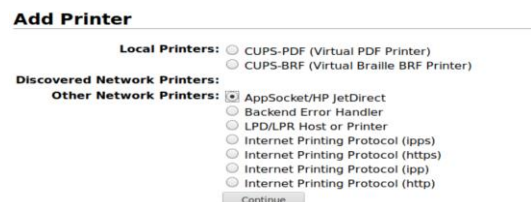


Fig 12.3 ingreso impresora nueva

El socket será la dirección a configurar en la maquina cliente

Add Printer

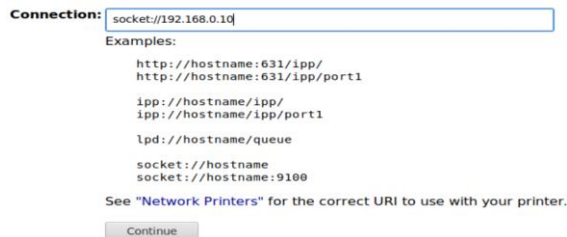


Fig 12.4 Socket de conexión

Add Printer

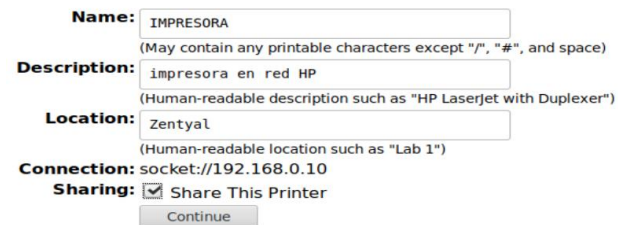


Fig 12.5 parámetros de conexión impresora

Se dejan las opciones por defecto y el driver de impresión se escoge el indicado en la imagen.

IMPRESORA (Idle, Accepting Jobs, Shared)

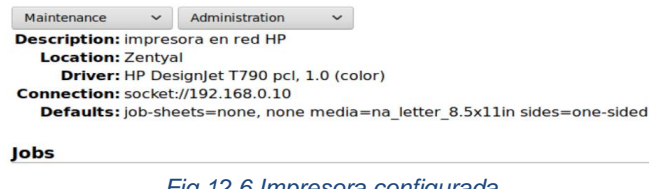


Fig 12.6 Impresora configurada

Configuro la escucha de los puertos

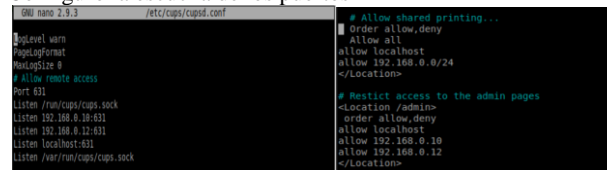


Fig 12.7 habilitar escucha de puertos

Configuración en el equipo cliente

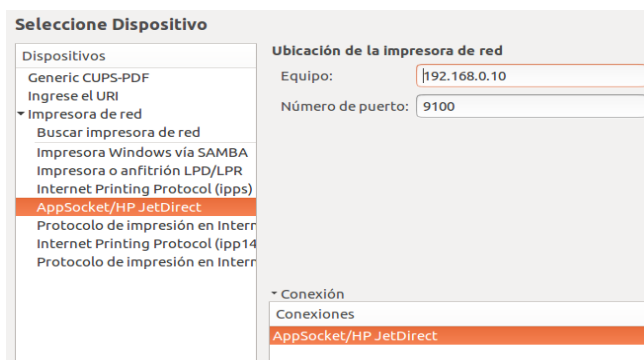


Fig 12.8 Configuración impresora equipo cliente

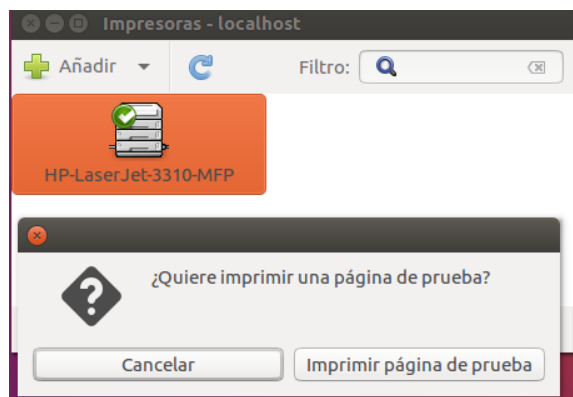


Fig 12.9 impresora lista

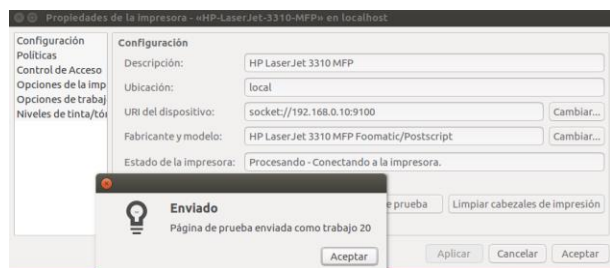


Fig 11.12 prueba de impresión

Fin de configuración de impresora.

E- Temática 5: VPN

Esta temática fue desarrollada por el Estudiante Luis Fernando Muriel Delgado.

Para el desarrollo de esta temática se descargan los siguientes módulos:

VPN: para crear el túnel privado.

Autoridad de certificación: para crear los certificados del servidor, de la vpn y de los equipos que se van a conectar.

Firewall: Para habilitar los puertos que se necesitan.



Fig 12 activación modulo VPN

Primero se deben generar los certificados necesarios para la VPN, en este caso se crean 3 certificados, en el módulo *Autoridad de Certificación* --- *General*.



Fig 12.1 ingreso modulo VPN

El primer certificado, el cual es para el servidor.



Fig 12.2 configuración autoridad certificadora

El segundo certificado el cual es para la red VPN a crear.



Fig 12.3 configuración autoridad certificadora

El tercero el cual va a ser para la máquina cliente la cual se va a conectar a la VPN.



Fig 12.3 Certificado para equipo cliente

Tener en cuenta que por cada máquina que se vaya a conectar a la VPN se debe generar un certificado.

En el módulo *VPN – Servidores*, añadir un nuevo servidor.



Fig 12.4 añadir nuevos servidores

Asignar un nombre y deseleccionar la opción de *Habilitado*.



Fig 12.5 Añadir Servidor

Asignarle el certificado creado, identificar el puerto que será utilizado por la VPN,



Fig 12.6 asignación de certificado

Ir a la opción de *Red – Servicios*, añadir un nuevo servicio y configurarle el protocolo y el puerto de destino.



Fig 12.8 configuración puerto de conexión

En el cortafuegos crear una nueva regla para la red interna y configurarla.



Fig 13 añadir nueva regla de firewall



Fig 13 añadir nueva regla de firewall

Para conocer la ip pública de Zentyal se puede ingresa a la página <https://who.is>, en la cual se puede identificar.



Fig 13 Validar IP publica

Para identificar la ip de red local, se debe abrir la terminal y ejecutar el comando `ifconfig`.

```
fermuriel@zentyalpasoocho:~$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.0.32 netmask 255.255.255.0 broadcast 192.168.0.255
    ether 08:00:27:1c:d7:c2 txqueuelen 1000 (Ethernet)
    RX packets 1791 bytes 297154 (297.1 KB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 1160 bytes 109782 (109.7 KB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

Fig 13.1 Validación IP

En *Servidores VPN* ir a la opción *Descargar paquete de configuración de cliente*.

Ingresar el *tipo de cliente*, seleccionar el *Certificado del cliente* creado con anterioridad e ingresar las ip pública y local y descargar.



Fig 14 descargar certificado cliente

El archivo comprimido generado se le debe llegar a la persona que se va a conectar a la VPN, ya sea por medio del correo electrónico, usb, google drive, etc.

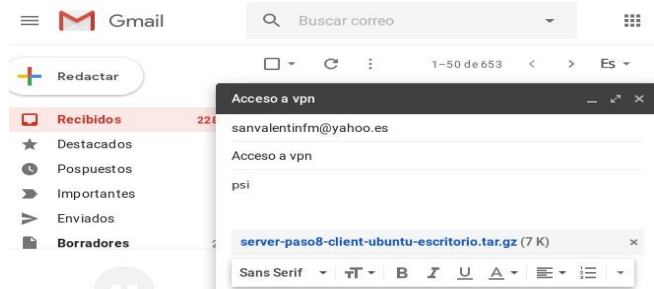


Fig 14.1 Envío de certificado a cliente

Para que se puede conectar el cliente, debe instalar la herramienta `openvpn`.

```
luis-muriel@luismuriel-VirtualBox: ~
luis-muriel@luismuriel-VirtualBox:~$ sudo apt-get install openvpn network-manager
-
openvpn-gnome
[sudo] password for luis-muriel:
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias
Leyendo la información de estado... Hecho
Los paquetes indicados a continuación se instalaron de forma automática y ya no s
on necesarios.
libdbusmenu-gtk4 liblvm3.0 libnrccommon5 libqmi-glib1 libqpdf17
ubuntu-core-launcher
Utilice «sudo apt autoremove» para eliminarlos.
Se instalarán los siguientes paquetes adicionales:
libpkcs11-helper1 network-manager-openvpn
Paquetes sugeridos:
easy-rsa
Se instalarán los siguientes paquetes NUEVOS:
libpkcs11-helper1 network-manager-openvpn network-manager-openvpn-gnome
openvpn
0 actualizados, 4 nuevos se instalarán, 0 para eliminar y 4 no actualizados.
Se necesita descargar 671 kB de archivos.
Se utilizarán 2,505 kB de espacio de disco adicional después de esta operación.
¿Desea continuar? [S/n] s
```

Fig 14.2 Instalación de openVPN

Descomprimir el paquete de configuración y copiar los archivos en la ruta: `/etc/openvpn` por medio de la terminal.

```
luis-muriel@luismuriel-VirtualBox: ~/Descargas
luis-muriel@luismuriel-VirtualBox:~/Descargas$ sudo mv ubuntu-escritorio.pem ser
ver-paso8-client.conf DA87E57879223E5C.pem cacert.pem /etc/openvpn
luis-muriel@luismuriel-VirtualBox:~/Descargas$
```

Fig 14.3 configuración de archivos

Ejecutar el comando: `sudo openvpn--config /etc/openvpn/archivo de configuración`.

```
luis-muriel@luismuriel-VirtualBox: /etc/openvpn
] [EPOLL] [PKCS11] [MH] [IPv6] built on Jun 22 2017
Tue Dec 11 01:33:55 2018 library versions: OpenSSL 1.0.2g 1 Mar 2016, LZO 2.08
Tue Dec 11 01:33:55 2018 WARNING: file 'ubuntu-escritorio.pem' is group or other
s accessible
Tue Dec 11 01:33:55 2018 Socket Buffers: R=[212992->212992] S=[212992->212992]
Tue Dec 11 01:33:55 2018 UDPv4 link local: [undef]
Tue Dec 11 01:33:55 2018 UDPv4 link remote: [AF_INET]192.168.0.32:1194
Tue Dec 11 01:34:56 2018 TLS Error: TLS key negotiation failed to occur within 6
0 seconds (check your network connectivity)
```

Fig 14.4 configuración openVPN

El cliente ya puede ingresar a la vpn creada y habilitada.



Fig 14.5 OpenVPN habilitado.

CONCLUSIONES

- ✓ La configuración DHCP nos permite gestionar el direccionamiento ip y la distribución del nombre de dominio junto con la configuración DNS del computador Zentyal a los equipos clientes. Adicionalmente el DNS traduce la dirección ip del servidor en palabras y el controlador de dominio nos permite regular y administrar la distribución de una red informática para compartir servicios y ajustados a los parámetros de una configuración específica.
- ✓ Por medio de la actividad realizada se llevó a cabo la configuración de proxy no transparente configurando listas blancas y negras bajo Zentyal para denegar o permitir el acceso a páginas de internet de un equipo cliente Ubuntu, comprendiendo los conceptos clave del tema.
- ✓ Se fortalecieron nuestros conocimientos y afinamos aún más en el entorno de trabajo GNU/Linux, implementado soluciones para las tareas reglas de denegación de contenidos Web para nuestro caso redes sociales tales como: Facebook, YouTube, Instagram, Twitter, configurando sistemas de cortafuegos en GNU/Linux lo que nos permitió denegar el acceso a las webs mencionadas, lo que conlleva a consultar, investigar y poner en práctica cada tema de manera que así cumplimos satisfactoriamente con los objetivos de la actividad final curso.
- ✓ Por medio de Zentyal se puede establecer un recurso compartido multiplataforma al cual se accedió con un usuario del Directorio Activo y por medio de las Listas de Control de Acceso se establecieron los permisos que el usuario tendría para utilizar esos recursos compartidos, Estableciendo de esta forma un servidor de archivos y servidor de impresión accesibles desde los equipos clientes.
- ✓ Zentyal incorpora una variedad de herramientas y entre ellas se encuentra la incorporación de VPN, con la cual se puede estableció una conexión segura entre un equipo cliente fuera de la red y los equipos o servidores que brindan servicios a dichos equipos de una forma segura y estable por medio de certificados que dan plena autenticación entre los dispositivos involucrados.

REFERENCIAS

- [1] Alvarez, A. A. (2013, 12 1). *practica 3 Firewall Zentyal*. From <https://www.youtube.com/watch?v=Mq62TEhTono>
- [2] Chacón, J. I. (n.d.). *Instalación y gestión de impresoras desde CUPS*. From http://ies.villablanca.madrid.educa.madrid.org/web2014/wordpress/informatica/wp-content/uploads/sites/16/2015/05/Trabajo_impresoras-CC-Jose_-Ignacio_Mardomingo.pdf
- [3] Documentation, U. O. (n.d.). *CUPS - Print Server*. From <https://help.ubuntu.com/lts/serverguide/cups.html.en>
- Ecured. (n.d.). *Zentyal*. From <https://www.ecured.cu/Zentyal>

- [4] KnowITFree. (2016, 10 6). *How to join Ubuntu 16.04 TLS to Active Directory Created in zentyal 4.2 Server*. From <https://www.youtube.com/watch?v=oNCzh3dkdBm>
- [5] Lema, A. d. (2016). *Configuración do firewall en Zentyal [Archivo de video]*. From <https://www.youtube.com/watch?v=kESyHFFoX-E>
- [6] Open, P. (2018, 11 9). *Download PowerBorker*. From <https://www.beyondtrust.com/powerbroker-identity-services-open-request/>
- [7] UnderPro. (2014). *Zentyal Primeros Pasos Configurar Tarjetas de Red en un servidor real Parte 2 [Archivo de video]*. *Recuperado de:*. From <https://www.youtube.com/watch?v=5R8cvV17V9s>; <https://www.youtube.com/watch?v=5R8cvV17V9s>
- [8] Wiki, Z. (2017). *Es/4.1/Apéndice A: Escenarios avanzados de red*. *Recuperado de:* . From https://wiki.zentyal.org/wiki/Es/4.1/Apendice_A:_Escenarios_avanzados_de_red
- [9] zentyal.org. (2015, 4 22). *Es/4.1/Instalacion*. From <https://wiki.zentyal.org/wiki/Es/4.1/Instalacion>