

Gestión e implementación de servicios IT para intranet y extranet, bajo Zentyal Server

Yury Duarte Sánchez, Andrea Cecilia Forero, Sergio Andrey Reyes Fandiño, Andrea Yulieth Forero Ledesma
ECBTI, UNAD

Colombia

yyduartes@unadvirtual.edu.co
aforeroal@unadvirtual.edu.co
unadestudio11@gmail.com
anyufole@gmail.com

RESUMEN: Con el presente artículo se pretende plasmar una observación y una caracterización de los diferentes conceptos fundamentales de los sistemas operativos GNU/LINUX, haciendo uso y organización de aportes realizados durante el curso, con los cuales el estudiante profundizará acerca de los pasos y temáticas presentados, logrando de esta manera alcanzar mayor comprensión y desarrollar habilidades en la optimización de las diferentes herramientas que nos ofrece GNU/LINUX.

PALABRAS CLAVE: GNU/LINUX, Ubuntu, server, máquina virtual, Proxy, Puerto, DNS, DHCP, Vpn.

I. INTRODUCCIÓN

En el trayecto del presente curso se expusieron las herramientas para la administración del sistema operativo GNU/LINUX, creando un entorno de servidores con su instalación, configuración y administración avanzada, también se abarcó a grandes rasgos la seguridad de sistemas GNU/LINUX y la implementación de aplicaciones y contenidos web.

Con a lo anterior en el paso 8 del curso, se aplicaron y profundizaron los conocimientos adquiridos en las fases anteriores.

A continuación, se realizará un análisis de las siguientes temáticas:

Temática 1: DHCP Server, DNS Server y Controlador de Dominio.

Temática 2: Proxy no transparente

Temática 3: Cortafuegos

Temática 4: File Server y Print Server

Temática 5: VPN

II. TEMÁTICA 1

SERVIDOR DHCP

Posterior a la configuración básica del servidor Zentyal 5.0, se da inicio al desarrollo de la primera de las 5 temáticas propuestas. El servidor DHCP es una herramienta cuya función principal es distribuir direcciones IP en una red, para lo anterior es necesario que el servidor Zentyal este configurado con una IP fija, con el fin de que cuando la máquina cliente realice la primera transmisión de paquetes, ésta última obtenga la configuración de red que fue asignada en un rango de IP's

dentro del servidor Zentyal, posiblemente sea necesario hacer una configuración en el archivo de interfaces de red o a través del network manager un par de líneas para dar a entender la máquina cliente que su salida a la red será a través de DHCP.

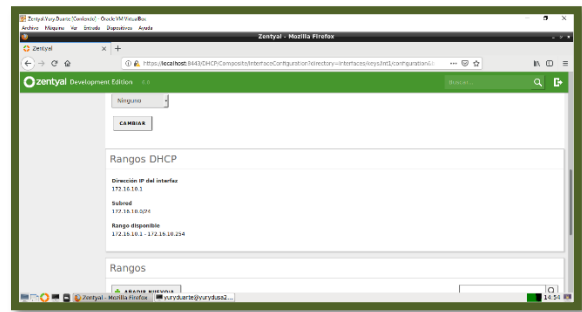


Figura 1. Configuración de rangos de IPs

SERVIDOR DNS

Un servidor DNS o sistema de nombres de dominio, se encarga de traducir nombres de dominio a Ip's y viceversa; en la actividad realizada con el servidor Zentyal 5.0, éste último se configura como un servidor de Dominio a través de una de las interfaces de red creadas en el momento de la instalación la cual cuenta con una Ip fija. La máquina cliente (Ubuntu) debe ser configurada para que use como "nameserver", la Ip de la máquina Zentyal y por la cual también tendrá salida a la red.

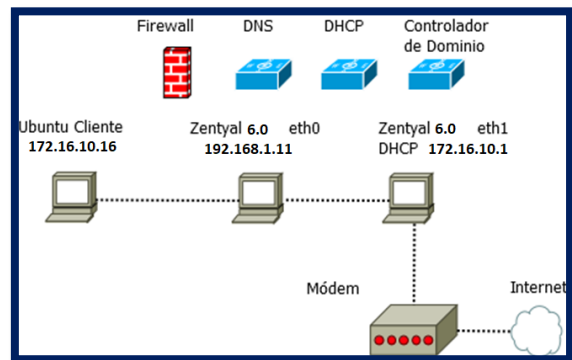


Figura 2. Arquitectura de la temática

CONTROLADOR DE DOMINIO

Zentyal es un servidor altamente versátil, el cual también proporciona una utilidad para hacer un control de las máquinas

que ingresan al dominio, en el momento de la instalación del Servidor éste configura por defecto un nombre dominio (el cual puede ser modificado), con un usuario Administrador por defecto el cual puede ser utilizado para ingresar a Zentyal desde un cliente; por el lado del cliente bien sea Windows o Linux, es necesario hacer unas configuraciones, para éste caso puntual si es Ubuntu Desktop, existe una herramienta muy útil controlada por terceros llamada LikeWise, con la cual a través de modo gráfico o por consola es posible añadir la máquina cliente al dominio Zentyal de una manera no tan compleja, siempre y cuando no se presenten problemas con restricciones o deficiencias en la configuración mandataria.

III. TEMÁTICA 2

PROXY NO TRANSPARENTE

Para empezar, debemos conocer la diferencia entre un proxy transparente y uno no transparente, en el caso del no transparente se requiere especificar la IP del servidor proxy y el puerto para su uso puntualmente para esta actividad sería el puerto 3128, para el proxy transparente como lo indica su nombre es transparente para el usuario y no se requieren datos de IP ni puerto.

Zentyal nos permite centralizar servicios básicos como lo son DNS, DHCP, FTP, y WEB, y mediante ellos implementar los niveles de seguridad adecuados a la red.

El proxy va actuar como punto intermedio entre los equipos de cómputo con los que cuenta la red y el o los servidores a los que se desean acceder por medio de cada equipo. Se debe tener en cuenta las características básicas para esta implementación como por ejemplo el espacio de 10 GB para la caché, dependiendo de las páginas que se desean bloquear se debe evaluar si es necesario utilizar un proxy no transparente ya que este bloqueara los sitios para cada IP y no de manera general. De esta manera se permitirá o denegará el acceso web según el contenido que considerará para cada equipo. Configuramos el proxy, desde las opciones de internet, con la IP 192.168.0.3 y el puerto 3128.

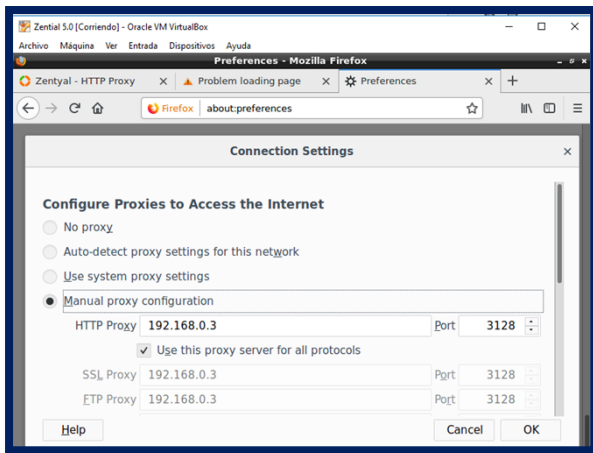


Figura 3. Configuración del proxy por medio de IP y puerto.

Ingresamos la URL de una página, y notamos que no podemos acceder a ella por la configuración que hicimos del proxy.

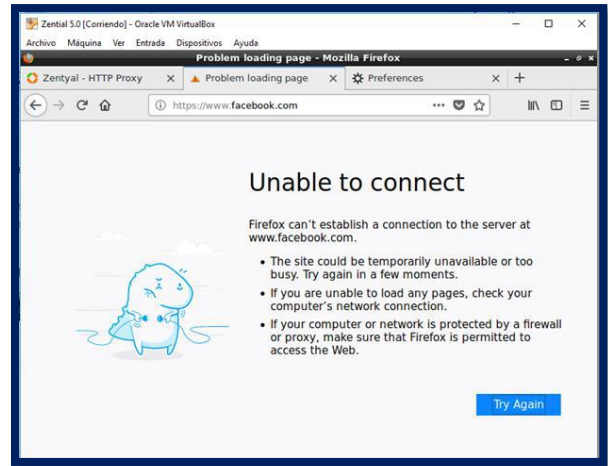


Figura 4. Acceso denegado a internet por medio de IP y puerto.

IV. TEMÁTICA 3

CORTAFUEGOS

Un cortafuego (o firewall en inglés) se trata de un software que controla las conexiones que se realizan a internet desde o hasta tu ordenador.

El modelo de seguridad de Zentyal se basa en intentar proporcionar la máxima seguridad posible en su configuración predeterminada, intentando a la vez minimizar los esfuerzos a realizar tras añadir un nuevo servicio.

Encontramos varios tipos de reglas de filtrado que el firewall de zentyal nos proporciona según las necesidades de nuestra red.

- Reglas de filtrado desde las redes internas a zentyal
- Reglas de filtrado para las redes internas
- Reglas de filtrado para el tráfico saliente de zentyal
- Reglas de filtrado desde las redes externas a zentyal
- Reglas de filtrado desde las redes externas a las internas.

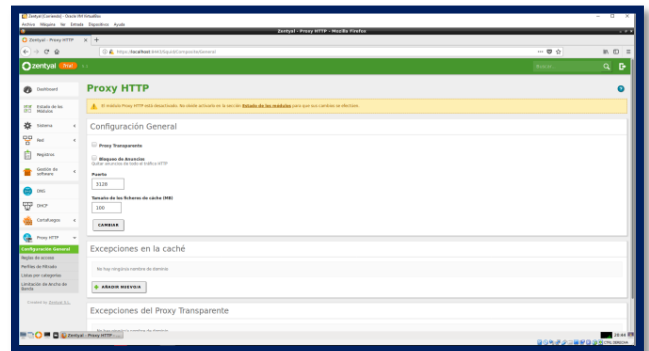


Figura 5. Configuración general del servidor proxy.

Estas políticas de acceso se implementan para varios segmentos de red, estos segmentos y su tráfico serán controlados por estas reglas como lo es el tipo de protocolo el puerto de origen y el destino.

Se configura las interfaces de red eth0 y eth1 para que Zentyal pueda establecer las reglas de filtrado sobre estas redes asignándole así una ip a nuestro Ubuntu desktop.

Zentyal contiene un módulo de Proxy HTTP que nos permite crear perfiles de filtrado, estos se pueden generar por ejemplo para perfiles empresariales y así controlar su navegación. Cada perfil tiene sus reglas de filtrado y es allí donde se establecen las reglas de dominios y urls, adicional a eso se cuenta con un umbral de filtrado de contenido que nos indica cuan estricto es el filtro, entre ellos encontramos muy permisivo, permisivo, medio, estricto y muy estricto. En el Proxy HTTP tenemos reglas de acceso que nos permite crear un periodo de tiempo en el cual se aplica esta regla, se marca origen y decisión.

Se bloquean ciertas páginas web y redes sociales tanto para un grupo de usuario como por ip o por dominio.

De esta forma tenemos un Firewall Zentyal activado y configurado de forma muy básica. A partir de aquí será cuestión de saber lo que queremos hacer en nuestra red, y entonces construir los tipos de sentencias adecuadas para permitir o bloquear el tráfico deseado en cada caso.

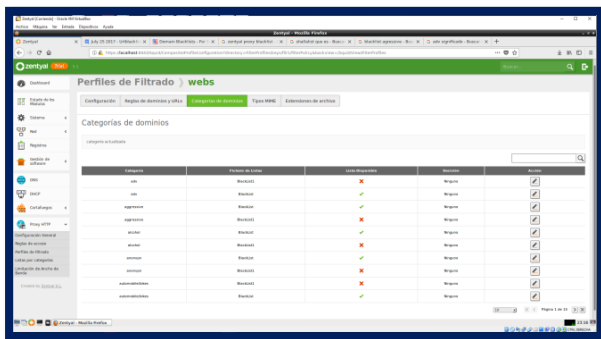


Figura 6. Categorías de sitios web para filtrado.

V. TEMÁTICA 4

FILE SERVER Y PRINT SERVER

Este es un servicio que posee Zentyal para poder convertir un equipo en un servidor de ficheros (file server). Esto se puede hacer por medio de la configuración de un controlador de dominio del mismo Zentyal y así dentro de este poder tener usuarios del dominio para darle acceso a los ficheros compartidos, estos permisos se pueden dar de completa administración, escritura o lectura y se puede dar ya sea a un usuario o más o por medio de grupos si se manejan en grandes cantidades.

Para adelantar esta temática, se realiza la instalación del SO Zentyal 5.0 (en la parte de la instalación se configura la interfaz de red con el segmento que esta el Ubuntu que es el que se agrega al dominio) y la configuración e activación del servicio de Controlador de Dominio y compartición de ficheros, para esto se crea un dominio con su respectivo nombre (el que le queramos colocar), se crea usuario de dominio.

Después de esto se realiza la inclusión del Ubuntu al dominio creado, para esto se deja como DNS la ip configurada en el Zentyal, se instala el likewise y por medio este se realiza la conexión del equipo, después de esto el equipo ya queda habilitado para ingresar con el usuario creado en el dominio y tener permisos a los ficheros compartidos que se le asignaron. Ya cuando se ingresa al equipo con el usuario del dominio instalamos samba en Ubuntu y buscamos la ruta compartida que se generó desde Zentyal.

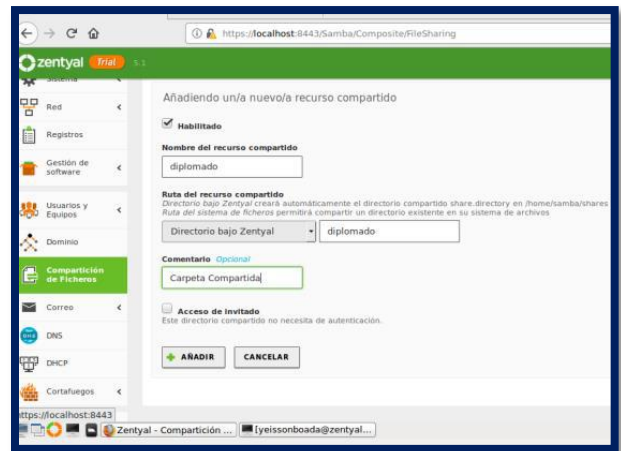


Figura 7. Configuración de carpeta compartida.

VI. TEMÁTICA 5

VPN

Una VPN es una tecnología de red que se utiliza para conectar uno o más computadores a una red privada utilizando internet.

Las compañías suelen usar las VPN para que sus integrantes puedan desde sus casas o cualquier sitio con acceso a internet, acceder a recursos corporativos que de otro modo no podrían. Aunque esta es una de las muchas funciones que posee una VPN.

La versión de Linux Zentyal usada para realizar la creación del servidor VPN fue la 5.0, luego de la instalación y configuración inicial del sistema operativo Linux Zentyal, procedemos a la creación de nuestro servidor VPN. El servidor VPN antes de su creación necesita un Certificado de la Autoridad de Certificación (CAC) Zentyal nos permite la creación de este certificado y anexo a la creación de nuestro servidor VPN.

El servidor VPN solo debe ser configurado con dicho certificado, se debe habilitar la interfaz TUN para permitir el túnel y permitir conexiones cliente-cliente para poder comunicar equipos clientes.

Es necesario que para cada cliente que se conectara a nuestro servidor VPN se genere un certificado, Zentyal nos permite crear estos certificados dándoles un nombre y unos días de duración.

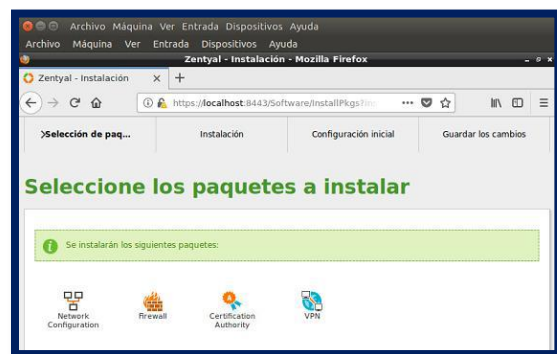


Figura 8. Selección de servicios a instalar.

Linux Zentyal nos permite descargar un paquete de configuración de cliente el cual tiene en su interior archivos .pm y el archivo de configuración que nos permite realizar la conexión a nuestro servidor VPN.

Dicha conexión se realiza gracias a sistemas como Open VPN o Tunnelblick este tipo de software nos permite cargar los archivos de configuración del paquete de configuración para realizar la conexión al servidor VPN.

Para realizar una conexión remota a un equipo perteneciente a la red VPN este equipo debe estar encendido, nuestro servidor VPN debe estar habilitado y encendido además que el equipo emisor y receptor deben estar conectados a nuestro servidor VPN, esta conexión remota se realiza en caso de Windows desde su funcionalidad conexión a escritorio remoto que nos permite ingresar la IP de nuestro equipo destino, dicha IP no la otorgara nuestro servidor VPN.

De esta forma se crea un servidor VPN bajo Linux Zentyal y se realiza la conexión remota de dos equipos.

Se instalan los paquetes para la configuración de nuestro servicio vpn. La instalación de los paquetes termina con éxito. Para configurar el servicio VPN lo primero que nos pide es generar un certificado de autoridad

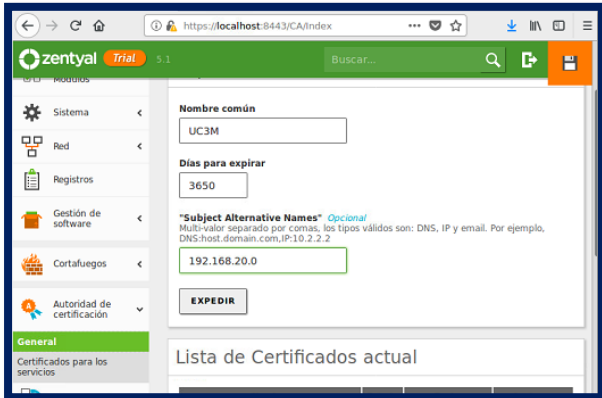


Figura 9. Generación de certificado de autoridad.

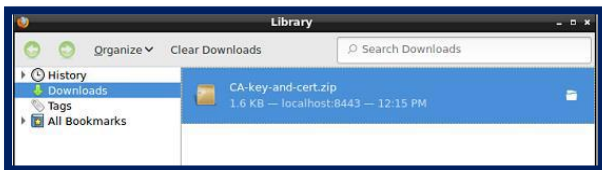


Figura 10. Certificado de autoridad.

VII. CONCLUSIONES

Este trabajo final nos permitió conocer e interactuar con las excelentes características de Zentyal Server para la administración, configuración e implementación de los servicios de red que puede tener una empresa. Con ayuda del servidor Zentyal se realizaron configuraciones con el servidor Proxy HTTP que cuenta con módulos necesarios para el correcto funcionamiento de dicho servicio. En la administración de TI, el proxy no transparente nos permitió aumentar la seguridad.

Se concluye que por medio de un controlador de dominio se puede manipular en una organización de manera más rápida usuarios, grupos, recursos compartidos.

Dar permisos como sea requerido en ficheros compartidos ya sea a un solo usuario o grupos creados e ingresando el usuario que le queramos dar estos permisos.

Podemos agregar equipos al controlador de dominio para que desde estos podamos acceder a los usuarios creados en el dominio y así poder tener accesos a los recursos compartidos. Se evidencia que estos recursos que se comparten se realizan por medio de samba.

En esta versión que se realizó la instalación Zentyal 5.0.

VIII. REFERENCIAS

- [1] Zentyal Community. (2017). Es/5.0/Instalacion. 05/2018, de Zentyal Community Sitio web: <https://wiki.zentyal.org/wiki/Es/5.0/Instalacion#el-instalador-de-zentyal>.
- [2] Zentyal Community. (2004). Usuarios, Equipos y Compartición de ficheros. 05/2018, de Zentyal Community Sitio web: <https://doc.zentyal.org/es/directory.html>.
- [3] Ubuntu Documentation. (2011). CUPS - Print Server. 05/2018, de Ubuntu Documentation Sitio web: <https://help.ubuntu.com/lts/serverguide/cups.html.en>.
- [4] Es/5.0/Servicio de Proxy HTTP - Zentyal Linux Small Business Server. 05/2018. Sitio web https://wiki.zentyal.org/wiki/Es/5.0/Servicio_de_Proxy_HTTP
- [5] Zentyal Server | Zentyal. 05/2018. Sitio web <http://www.zentyal.com/es/zentyal-server/>
- [6] HTTPS con proxy NO transparente. (2018). Sitio web <https://forum.zentyal.org/index.php?topic=7298>
- [7] Zentyal - Configurar Proxy Web HTTP No Transparente. 05/2018. Sitio web <https://www.youtube.com/watch?v=PG7pcYmBkw4>