

Implementación de infraestructura TI usando el servidor Zentyal

Gina Camelo Almanza, Walter Fandiño, Yeimmy Paola Camargo, Diego Guerrero, Cristian Perdomo

Universidad Nacional Abierta y a Distancia UNAD

Bogotá, Colombia

gpcamelo@unadvirtual.edu.co

wfandinos@unadvirtual.edu.co

ypcamargous@unadvirtual.edu.co

dmguerrero@unadvirtual.edu.co

cperdomoe@unadvirtual.edu.co

II. DESARROLLO DE LAS TEMÁTICAS

Resumen: Este proyecto está enfocado en solventar las necesidades tecnológicas de pequeñas y medianas empresas, haciendo uso de la herramienta Zentia, en el proyecto final de la opción de grado diplomado en Linux, fueron desarrolladas 5 temáticas enfocadas a la solución tecnológica de infraestructura con la herramienta Zentia en la versión 5.0, distribución Linux que permite la implementación de diferentes servidores con la misma plataforma, en esta actividad se realizó el proceso de instalación, configuración y pruebas para el uso de servidores, DNS, DHCP, VPN, Impresoras, File Server, Proxy no Transparente, Cortafuegos.

Se comprobó que para el correcto funcionamiento del servidor DHCP se requiere tener las MAC de los equipos, para el servidor VPN se deben crear certificados por usuario, para el zentia y para el servidor, en el cortafuegos se puede dar acceso o denegar acorde a lo que se requiera, la metodología con la cual se desarrolló esta actividad incluyó la configuración en Virtual box con doble tarjeta de red.

Palabras Claves: Zentia, DNS, DHCP, VPN, File Server, Proxy no Transparente, Firewall.

Abstract—This project is focused on the technological needs of small and medium enterprises, making use of the Zentia tool, in the final project of the diploma option in Linux, it was developed 5 early focused on the infrastructure technological solution with the Zentia tool in version 5.0, Linux distribution that allows the implementation of different servers with the same platform, in this activity the installation process was performed, and tests for the use of servers, DNS, DHCP, VPN, Printers, File Server, Proxy not Transparente, Firewall.

It was verified that for the correct functioning of the DHCP server it is required to have the MACs of the equipment, for the VPN server certificates must be created per user, for the remote server and for the server, it can be given access or denied according to what is require, the methodology with which this activity can be done in the application virtual box with a double red card.

Keys word: Zentia, DNS, DHCP, VPN, File Server, Proxy not

A. 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 Zentia.

Solución planteada: Para dar solución a esta temática, se configura el DHCP server y el DNS Server:

Para configurar el DHCP Server, vamos a la máquina de Zentia instalada, ingresamos al panel de control, ingresamos al Dashboard, y en Red, Interfaces de red y en la primera red configuramos la red interna, habilitamos la opción Externo (WAN), damos clic en cambiar.

Interfaces de Red

The screenshot shows the 'Interfaces de Red' configuration page in Zentia. At the top, there are two tabs: 'eth0' (selected) and 'eth1'. Below the tabs, there is a form for configuring the selected interface. The 'Nombre' field contains 'eth0'. The 'Método' dropdown menu is set to 'DHCP'. There is a checked checkbox for 'Externo (WAN)' with a sub-note: 'Marque aquí si está usando Zentia como gateway y este interfaz está conectado a su router a Internet'. At the bottom of the form is a 'CAMBIAR' button.

Fig. 1 Configuración interfaz de red eth0

En la segunda interfaz vamos a configurar con la IP 192.168.0.21 y damos clic en cambiar.

Abrimos la consola y hacemos ping a la dirección asignada a la máquina de Ubuntu y en la máquina virtual de Ubuntu realizamos ping a la dirección Ip asignada a Zentia Server.

Transparent, Firewall.

I. INTRODUCCIÓN

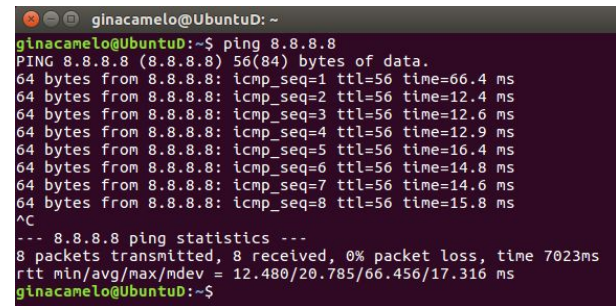
En la actualidad las empresas están en la necesidad, de ir de la mano de los avances tecnológicos y garantizar que la productividad de esta sea cada vez mayor, para esto no solo se debe contar con la persona adecuada para desempeñar con excelencia sus funciones, si no tener todos los equipos y conexiones necesarias, que funcionen de forma adecuada para desempeñar su trabajo y que las probabilidades de pérdida de información o caídas de la red sean nulas.

Para dar solución a la problemática identificada, se realiza la administración y control de Zentyal, para implementar servicios de infraestructura IT de mayor nivel para intranet y extranet.

Con Zentyal es posible administrar todos los servicios de una red informática en una sola plataforma, en una empresa Pyme. Linux creo Zentyal para poder tener un acercamiento directo a las medianas empresas, ya que este tipo de empresa, no ha estado muy considerado dentro de los desarrollos de servidores, se han realizado soluciones para grandes empresas que al implementar esta misma solución para una Pyme son pocas las probabilidades por su costo y tiempo de implementación.

En el presente artículo vamos a dar a conocer una solución de código abierto, que administra los servicios de una red informática, como son el acceso a internet, seguridad en la red y en la transferencia de archivos e infraestructura, su interfaz es sencilla de manejar y configurar. En Zentyal se va a configurar el DHCP server, DNS server y controlador de dominio, proxy no transparente, cortafuegos, file server y print server, VPN.

Ingresamos a la máquina de Ubuntu y en la consola, damos ip a s para confirmar el direccionamiento a la IP. Hacemos ping a la dirección 8.8.8.8 y verificamos conexión. Ingresamos al navegador y en este caso ingresamos a la página de Gmail, ingresa correctamente.



```
ginacamel@UbuntuD: ~  
ginacamel@UbuntuD:~$ ping 8.8.8.8  
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data:  
64 bytes from 8.8.8.8: icmp_seq=1 ttl=56 time=66.4 ms  
64 bytes from 8.8.8.8: icmp_seq=2 ttl=56 time=12.4 ms  
64 bytes from 8.8.8.8: icmp_seq=3 ttl=56 time=12.6 ms  
64 bytes from 8.8.8.8: icmp_seq=4 ttl=56 time=12.9 ms  
64 bytes from 8.8.8.8: icmp_seq=5 ttl=56 time=16.4 ms  
64 bytes from 8.8.8.8: icmp_seq=6 ttl=56 time=14.8 ms  
64 bytes from 8.8.8.8: icmp_seq=7 ttl=56 time=14.6 ms  
64 bytes from 8.8.8.8: icmp_seq=8 ttl=56 time=15.8 ms  
^C  
--- 8.8.8.8 ping statistics ---  
8 packets transmitted, 8 received, 0% packet loss, time 7023ms  
rtt min/avg/max/mdev = 12.480/20.785/66.456/17.316 ms  
ginacamel@UbuntuD:~$
```

Fig. 6 Ping a la dirección 8.8.8.8 en Ubuntu Desktop

Controlador de dominio:

Ingresamos a Dominio y habilitamos perfiles móviles, damos clic en cambiar y en guardar cambios.

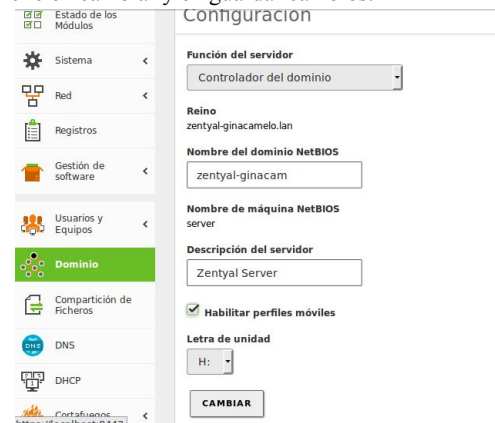
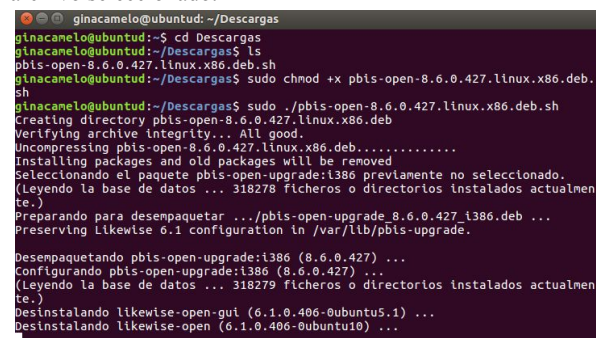


Fig. 7 Configuración controlador de dominio

Vamos a usuarios y equipos, damos clic en gestionar. Seleccionamos Users y damos clic en el botón más, añadimos un nuevo usuario, establecemos nombre, contraseña y en grupo seleccionamos Domain Admins, damos clic en añadir.

Ingresamos a la máquina virtual de Ubuntu Desktop. En el explorador ingresamos a la dirección <https://github.com/BeyondTrust/pbis-open/releases> y seleccionamos el archivo correspondiente, según la distribución. Damos clic en guardar archivo. En la consola ingresamos a la carpeta de descargas y digitamos los siguientes comandos para el archivo seleccionado.



```
ginacamel@ubuntu: ~/Descargas  
ginacamel@ubuntu:~$ cd Descargas  
ginacamel@ubuntu:~/Descargas$ ls  
pbis-open-8.6.0.427.linux.x86.deb.sh  
ginacamel@ubuntu:~/Descargas$ sudo chmod +x pbis-open-8.6.0.427.linux.x86.deb.sh  
ginacamel@ubuntu:~/Descargas$ sudo ./pbis-open-8.6.0.427.linux.x86.deb.sh  
Creating directory pbis-open-8.6.0.427.linux.x86.deb  
Verifying archive integrity... All good.  
Uncompressing pbis-open-8.6.0.427.linux.x86.deb .....  
Installing packages and old packages will be removed  
Seleccionando el paquete pbis-open-upgrade:i386 previamente no seleccionado.  
(Leyendo la base de datos ... 318278 ficheros o directorios instalados actualmen  
te.)  
Preparando para desempaquetar .../pbis-open-upgrade_8.6.0.427_i386.deb ...  
Preserving Likewise 6.1 configuration in /var/lib/pbis-upgrade.  
Desempaquetando pbis-open-upgrade:i386 (8.6.0.427) ...  
Configurando pbis-open-upgrade:i386 (8.6.0.427) ...  
(Leyendo la base de datos ... 318279 ficheros o directorios instalados actualmen  
te.)  
Desinstalando likewise-open-gui (6.1.0.406-0ubuntu5.1) ...  
Desinstalando likewise-open (6.1.0.406-0ubuntu10) ...
```

Fig. 8 Configuración de Ubuntu Desktop para vincular a dominio en



Fig. 2 Configuración interfaz de red eth1

Confirmamos por medio de consola que la dirección Ip ha sido establecida. En estado de los módulos verificamos que DHCP está habilitado. Ingresamos a DHCP. Interfaces y damos clic en configuración, en opciones personalizadas, rangos y añadimos un nuevo rango.

Rangos

Añadiendo un/a nuevo/a rango

Nombre
gina DHCP

De
192.168.0.22

Para
192.168.0.100

+ AÑADIR CANCELAR

Fig. 3 Establecer rangos DHCP

Ingresamos a la máquina virtual de Ubuntu Desktop y automáticamente se asigna la dirección Ip. Revisamos en la máquina de Zentyal en el Dashboard y en Ip asignadas con DHCP, aparece la máquina de Ubuntu.

IPs asignadas con DHCP

Dirección IP	Dirección MAC	Nombre de máquina
192.168.0.32	08:00:27:95:35:71	ubuntutd

Fig. 4 Ip asignadas por DHCP

Para configurar el DNS Server ingresamos a DNS, y habilitamos el cache de DNS transparente, damos clic en cambiar y en guardar cambios.

DNS

Configuración cambiada

Configuración

Habilitar el caché de DNS transparente

CAMBIAR

Redireccionadores

No hay ningún/a redireccionador

+ AÑADIR NUEVO/A

Fig. 5 Configuración DNS

Luego de que se realice la instalación, digitamos el siguiente comando para unir al dominio creado en Zentyal, a través de domainjoin, sudo domainjoin-cli join zentyal-ginacamelan.gpcamelan. Digitamos la contraseña del usuario creado gpcamelan y nos da el proceso exitoso.

```
gincamelan@ubuntu: ~/Descargas
SUCCESS
You should reboot this system before attempting GUI logins as a domain user.
gincamelan@ubuntu:~/Descargas$ ^C
gincamelan@ubuntu:~/Descargas$ sudo /etc/init.d/lwmsd restart
[ ok ] Restarting lwmsd (via systemctl): lwmsd.service.
gincamelan@ubuntu:~/Descargas$ sudo domainjoin-cli join zentyal-ginacamelan.gpcamelan
Joining to AD Domain: zentyal-ginacamelan.lan
With Computer DNS Name: ubuntu.zentyal-ginacamelan.lan
gpcamelan@ZENTYAL-GINACAMELO.LAN's password:
Error: LW_ERROR_NOT_HANDLED [code 0x00009c51]
The authentication request could not be handled
gincamelan@ubuntu:~/Descargas$ sudo domainjoin-cli join zentyal-ginacamelan.gpcamelan
Joining to AD Domain: zentyal-ginacamelan.lan
With Computer DNS Name: ubuntu.zentyal-ginacamelan.lan
gpcamelan@ZENTYAL-GINACAMELO.LAN's password:
SUCCESS
You should reboot this system before attempting GUI logins as a domain user.
gincamelan@ubuntu:~/Descargas$
```

Fig. 9 Ping a la dirección 8.8.8.8 en Ubuntu Desktop

En Zentyal verificamos en computadores y se ve la máquina de

Zentyal

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.

Dado que un cortafuego o firewall se caracteriza por ser un procedimiento que permite la defensa que permite controlar el tráfico que existe sobre una red, el cual hace que todo el tráfico de información que sea de entrante o saliente, pasa por un sistema de reglas que permiten el filtrado de la información que viaja por la red.

El cortafuegos ofrece las siguientes reglas de filtrado:

- Filtrado para las redes internas
- Filtrado desde las redes externas
- Filtrado para el tráfico saliente
- Filtrado de redes internas

De acuerdo a un conjunto de reglas que son configuradas de acuerdo a la necesidad de la empresa puesto que establece una barrera entre las redes internas que están protegidas y las redes externas en las cuales se puede tener expuesta la información, sobre todo en la internet.

Se agregan las reglas para la negación de conexión a páginas de redes sociales.

Configurar reglas

Decisión	Origen	Destino	Servicio	Descripción	Acción
<input checked="" type="checkbox"/>	Cualquiera	104.244.42.1/32	Cualquier TCP	Bloqueo Twitter	<input checked="" type="checkbox"/> <input checked="" type="checkbox"/> <input checked="" type="checkbox"/>
<input checked="" type="checkbox"/>	Cualquiera	34.192.220.89/32	Cualquier TCP	Bloqueo Instagram	<input checked="" type="checkbox"/> <input checked="" type="checkbox"/> <input checked="" type="checkbox"/>
<input checked="" type="checkbox"/>	Cualquiera	104.154.127.0/32	Cualquier TCP	Bloqueo Spotify	<input checked="" type="checkbox"/> <input checked="" type="checkbox"/> <input checked="" type="checkbox"/>
<input checked="" type="checkbox"/>	Cualquiera	40.121.80.0/32	Cualquier TCP	Bloqueo Skype	<input checked="" type="checkbox"/> <input checked="" type="checkbox"/> <input checked="" type="checkbox"/>
<input checked="" type="checkbox"/>	Cualquiera	216.58.222.0/32	Cualquier TCP	Bloqueo Youtube	<input checked="" type="checkbox"/> <input checked="" type="checkbox"/> <input checked="" type="checkbox"/>
<input checked="" type="checkbox"/>	Cualquiera	157.240.6.0/32	Cualquier TCP	Bloqueo facebook	<input checked="" type="checkbox"/> <input checked="" type="checkbox"/> <input checked="" type="checkbox"/>
<input checked="" type="checkbox"/>	192.168.10.1/32	Cualquiera	Administración Web de Zentyal	--	<input checked="" type="checkbox"/> <input checked="" type="checkbox"/> <input checked="" type="checkbox"/>
<input checked="" type="checkbox"/>	Cualquiera	Cualquiera	Cualquiera	--	<input checked="" type="checkbox"/> <input checked="" type="checkbox"/> <input checked="" type="checkbox"/>

Fig. 11 Ejemplo de agregación de reglas para navegación de las terminales.

Se obtiene las ip's de los sitios web y luego se agregan para que no sea posible conectarse cuando desde un desktop realicen la solicitud. Se realiza la prueba tratando de ingresar a facebook.com

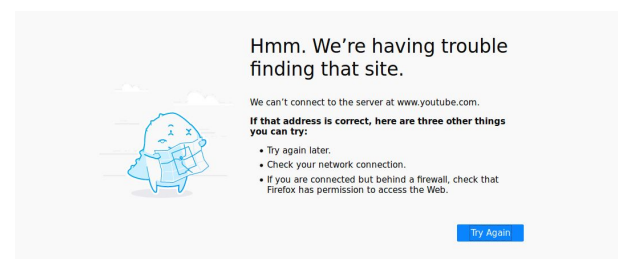


Fig. 12 Ejemplo de error de navegación Ubuntu desktop máquina virtual

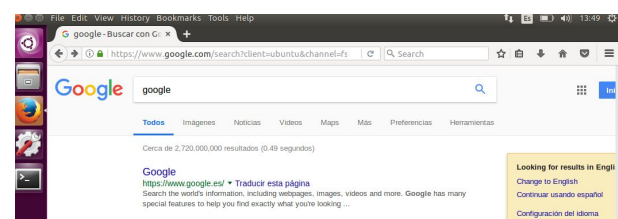


Fig. 13 Ejemplo de conexión de Ubuntu desktop.

Ubuntu asociada.



Fig. 10 Equipo Ubuntu vinculado al dominio en Zentyal

B. Temática 2: Proxy no Transparente.

Zentyal server brinda el servicio de controlar el acceso a internet por medio de un completo proxy, el cual permite realizar su gestión de forma implacable, desde crear perfiles de permisos hasta controlar tipos de archivos, Zentyal cuenta con una interfaz gráfica muy amigable en la que se puede restringir sitios web de forma eficiente y segura.

La principal característica del proxy no transparente es en el momento de su configuración en la máquina que se requiere realizar el control mediante el proxy, ya que se debe parametrizar especificando dirección ip del servidor y puerto.

C. Temática 3: Cortafuegos.

Producto esperado: implementación y configuración detallada para la restricción de la apertura de sitios o portales Web de

D. Temática 4: File Server y Print Server.

En esta sección se mostrará cómo realizar una estación de trabajo y de ficheros compartidos desde una máquina Ubuntu Desktop hacia un servidor Zentyal, utilizaremos un paquete de “BeyonTrust” llamado “pbis” para poder realizar la adición de dominio que nos garantiza la seguridad de control y el acceso a los recursos compartidos a otra máquina mientras esta se encuentre en el mismo dominio.

Lo anterior nos sirve para poder transferir archivos, compartir impresoras, adicionar carpetas compartidas y otras utilidades que se pueden crear desde una estación de trabajo.

Se creó el laboratorio evidenciando con capturas de pantalla y se realizó una demostración accediendo con un usuario creado desde Zentyal y accediendo con el mismo desde una máquina Ubuntu Desktop creando una carpeta compartida.

E. Temática 5: DNS.

El Configurar VPN en Zentyal cuenta con múltiples ventajas como: Cifrado basado en tecnología SSL, permite la conexión de clientes para Windows, Mac OS y Linux y autenticación mediante infraestructura de clave pública.

En este trabajo se desarrolló la implementación de una red privada con la ayuda del servidor Zentyal el cual permite la creación de diferentes servidores, y la gestión de servicios como DHCP,DNS,FIREWALL entre otros con los cuales se puede implementar toda la infraestructura requerida para una pequeña o mediana compañía.

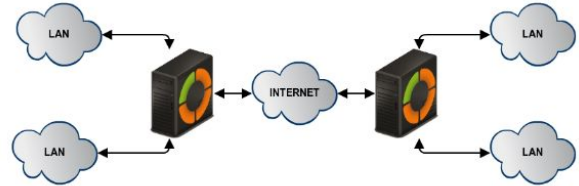


Fig. 14 Interconexión de redes VPN

Pasos para la correcta configuración de la VPN.

1. Crear un certificado para el servidor VPN
2. Crear certificado de la Autoridad de certificación
3. Instalar servicio VPN
4. Configurar servidor VPN
5. Verificar que se ha creado automáticamente un certificado para VPN en la AC
6. Crear un certificado para el servidor VPN
7. Verificar que se hayan creado los certificados y las llaves
8. Activar el servidor VPN
9. Verificar que el servidor VPN se ejecute correctamente
10. Configurar las opciones del servidor VPN
11. Configuración del cortafuego
12. Configuración de los certificados para los clientes
13. Instalación y configuración del cliente VPN

Se valida la conexión de datos.

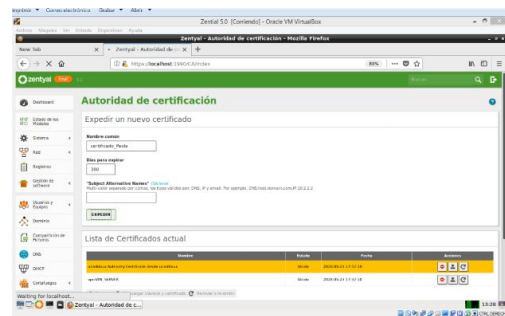


Fig. 15 Autoridad certificadora

Parametrización especial

1. Si se requiere que los clientes de VPN puedan conectarse entre sí usando dirección de VPN, para lo cual se debe activar la opción Permitir conexiones entre clientes en la sección de servidor.
2. Zentyal expide un certificado por defecto para el servidor, con el nombre vpn-<nuestronombrevpn>.
3. La forma más sencilla de configurar un cliente VPN es utilizando los bundles de Zentyal, paquetes de instalación que incluyen el archivo de configuración de VPN

Resultados:

1. En la implementación de la VPN fue requerido crear certificados para el sistema operativo y certificado de autenticación para el servidor, en este punto fue importante parametrizar desde que IP accedería el cliente y el tiempo de validez de los certificados.
2. El uso de VPN en una compañía permite utilizar de forma segura la infraestructura de red de Internet para ampliar su red interna ya que con la red privada se puede controlar el tráfico y asegurar varias características de seguridad como lo son la autenticación por usuario y la privacidad de la información.
3. En el proceso de investigación del funcionamiento e implementación de una VPN con zentyal se documentó que esta utiliza la estructura abierta de IPSec el cual es un marco de los estándares abiertos que proporciona la confidencialidad de los datos, la integridad de los datos, y la autenticación de datos y el cual ofrece funciones de seguridad para internet y para la creación de redes privadas seguras.

IV.CONCLUSIONES

1. Por medio de la configuración DHCP de Zentyal, es posible la asignación de Ip dinámicas según el rango establecido.
2. Con el controlador de dominio de Zentyal, se contrala los usuarios que pertenecen a una red, para administrar sus contraseñas y accesos que necesiten, según su cargo en el lugar de trabajo.
3. Mediante Zentyal se puede restringir el acceso a internet en una organización de forma efectiva y económica, por medio del proxy que nos brinda esta herramienta.

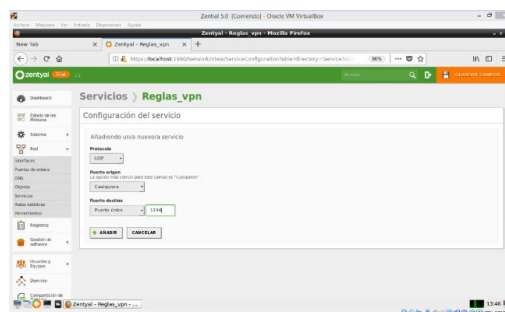


Fig. 16 Configuración de cortafuegos

REFERENCIAS

- [1] Official Zentyal Server Training | Zentyal
Website title: Zentyal.com
URL: <http://www.zentyal.com/training/>
- [2] Installation Guide - Zentyal Linux Small Business Server
Website title: Wiki.zentyal.org
URL: https://wiki.zentyal.org/wiki/Installation_Guide
- [3] Presentación
Website title: Wiki.zentyal.org
URL: <https://wiki.zentyal.org/wiki/Es/3.5/Presentacion>
- [4] How To Install Zentyal on Ubuntu 14.04 | DigitalOcean
Website title: Digitalocean.com
URL: <https://www.digitalocean.com/community/tutorials/how-to-install-zentyal-on-ubuntu-14-04>
- [5] BeyondTrust/pbis-open
Website title: GitHub
URL: <https://github.com/BeyondTrust/pbis-open/releases>
- [1] D. del Barrio. (2012). Firewall Zentyal. El Taller del Bit. [En línea]. Disponible en: <http://eltallerdelbit.com/firewall-zentyal>
- [6] Wiki.zentyal.org. (2017). Es/5.0/Cortafuegos - Zentyal Linux Small Business Server. [En línea] Disponible: <https://wiki.zentyal.org/wiki/Es/5.0/Cortafuegos>
- [7] Velosa Castañeda, J. C., Calvo Canizales, C. D., Riascos Castillo, E. M., Dajome Arizala, R. A., & Castro Alzate, F. J. (2018). Debatir, generar, determinar e implementar soluciones GNU/LINUX.
- [8] Jair Gómez Arias, [JGAITPro]. (2014, mayo 07). Zentyal - Instalar y configurar Proxy Web HTTP Transparente [Archivo de video]. Recuperado de <https://www.youtube.com/watch?v=X54YKfeFQhQ>
- [8] D. del Barrio. (2012). Firewall Zentyal. El Taller del Bit. [En línea]. Disponible en: <http://eltallerdelbit.com/firewall-zentyal>
- [9] Wiki.zentyal.org. (2017). Es/5.0/Cortafuegos - Zentyal Linux Small Business Server. [En línea] Disponible: <https://wiki.zentyal.org/wiki/Es/5.0/Cortafuegos>

4. De acuerdo a lo validado tras la instalación y configuración de firewall o cortafuegos se pudo determinar la importancia que ejerce sobre la red, la cual es bloquear los accesos a sitios web no autorizados así mismo permitir las conexiones autorizadas, dichas reglas pueden ser la restricción de ingreso a sitios, portales Web bien sea de entretenimiento o redes sociales.

5. Adicional a la función que cumple el cortafuego dentro de la red en donde está configurada, este proporciona un control y la forma de poder auditar el tráfico que haya en la red, lo cual para un administrador de redes es importante puesto que con esto puede evitar posibles ataques o indisponibilidad del servicio.