INSTALACION, ADMINISTRACION Y CONTROL DE SERVICIOS DE INFRAESTRUCTURA IT BAJO EL SISTEMA OPERATIVO ZENTYAL SERVER 5.0

Richard Andrés Zarama Nocua
e-mail: razaraman@unadvirtual.edu.co
Carlos Antonio Marín Lozano
e-mail: camarinlo@unad.edu.co
Ovidio Martínez Barco
e-mail: omartinezba@unadvirtual.edu.co
Jose Arley Betancourt
e-mail: josebr0321@hotmail.com
Alejandro Ramírez Inchima
e-mail: aramirezi@unadvirtual.edu.co

RESUMEN: *En el siguiente documento se evidenciará la instalación del sistema operativo Zentyal server en una máquina virtual basada en virtualbox para así poder administrar y controlar los servicios de infraestructura IT como son: DHCP Server, DNS Server y Controlador de Dominio, Proxy no transparente, Cortafuegos, File Server y Print Server y VPN.*

Además, el Zentyal server cuenta con una interfaz gráfica que es operativa desde la web lo que permite configurar sus servicios de acuerdo a las necesidades o requerimientos que se tengan en cualquier proyecto establecido.

PALABRAS CLAVE: Zentyal, DHCP, DNS, Proxy no transparente, Cortafuegos, File y Print Server, VPN.

1 INTRODUCCIÓN

Hoy en día se debe tener en cuenta que cualquier tipo de red informática sea en una empresa, en una microempresa, o en cualquier otro negocio se necesita en su estructura de seguridad algún tipo de filtro o algún tipo de control sobre esta, esto permite que se pueda manejar y administrar la información que se esté procesando, por lo tanto, es muy importante tener en cuenta que aquí es precisamente donde se hace necesario la implementación de los componentes de gestión y administración de la seguridad perimetral como lo son los cortafuegos, los proxys, las conexiones VPN, seguridad en la plataforma de correo, entre otros. Para este propósito se pueden usar herramientas de tipo hardware o software, siendo este último uno de los más usados por su bajo costo de implementación y sostenimiento, además de su versatilidad, permitiendo una mejora en la calidad de sus servicios con un control de seguridad de sus datos, por eso es aquí donde entra el Zentyal Server una de las tantas distribuciones que posee Linux en la cual se basa el desarrollo de las 5 temáticas establecidas en el paso 8 de este diplomado.

2 OBJETIVO

Formular soluciones con la implementación de cada una de las cinco Temáticas propuestas bajo GNU/Linux Zentyal Server, llevando a cabo la instalación, configuración y puesta en marcha de infraestructura tecnológica que permita dar respuesta a los requerimientos planteados.

3 DESARROLLO ACTIVIDAD

3.1 INSTALACIÓN ZENTYAL SERVER 5

Los siguientes requerimientos son los mínimos recomendados para un servidor de uso general con los patrones de uso normales:

Requisitos del hardware

Perfil de Zentyal	Usuarios	CPU	Memoria	Disco	Tarjeta Red
Puerta de acceso	<50 50 o mas	P4 o superior Xeon Dual Core o superior	2G 4G	80G 160G	2 o mas
Infraestructura	<50 50 o mas	P4 o superior	1G 2G	80G 160G	1
Oficina	<50 50 o mas	P4 o superior Xeon Dual Core o superior	1G 2G	250G 500G	1
Comunicaciones	<100 100 o mas	Xeon Dual Core o equivalente	4G 8G	250G 500G	1

Instalación y configuración

Pasos que se deben tener en cuenta para la instalación:

- Dirigirse a la página oficial de zentyal y descargar la imagen ISO.
- Crear una nueva máquina virtual Linux en virtualbox.

- Asignar tanto el espacio en disco duro como de memoria RAM.
- Crear dos adaptadores de red en la máquina virtual, una para red NAT y otra para red interna.
- Configurar la imagen ISO para que arranque con el inicio del nuevo sistema operativo
- Seleccionamos el idioma de instalación y nuestra ubicación de zona horaria.
- Configuramos la distribución del teclado a español
- Seleccionamos el adaptador de red principal en el cual va a configurarse zentyal
- Creamos un nuevo usuario para el sistema proporcionando nombre de usuario y contraseña.
- Seleccionamos la partición del disco duro en la cual se va a instalar zentyal
- Seleccionamos que la instalación sea con interfaz gráfica de usuario.
- El sistema pide reiniciarse para terminar con la instalación del sistema.
- Termina la instalación y nos solicita el serial para la activación del producto.
- En su primer uso la interfaz de usuario nos muestra un listado con los paquetes que se pueden instalar y configurar dentro de zentyal server como lo son: servicios de DHCP Server, DNS Server, Proxy, Cortafuegos, entre otros.
- Lego de seleccionar los paquetes requeridos inicia la instalación de los mismos.

3.2 TEMATICA 1 DHCP SERVER, DNS SERVER Y CONTROLADOR DE DOMINIO.

DHCP

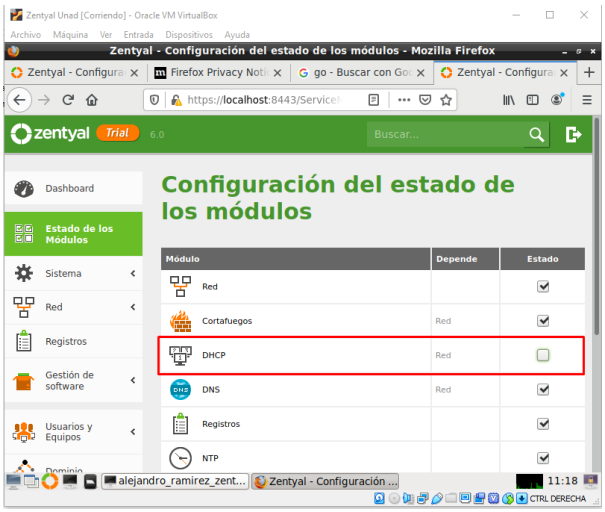
DHCP significa protocolo de configuración de host dinámico y es un protocolo de red utilizado en redes IP donde un servidor DHCP asigna automáticamente una dirección IP y otra información a cada host en la red para que puedan comunicarse de manera eficiente con otros puntos finales.

Además de la dirección IP, DHCP también asigna la máscara de subred, la dirección de puerta de enlace predeterminada, la dirección del servidor de nombres de dominio (DNS) y otros parámetros de configuración pertinentes. La solicitud de comentarios (RFC) 2131 y 2132 define DHCP como un estándar definido por IETF (Internet Engineering Task Force) basado en el protocolo BOOTP.

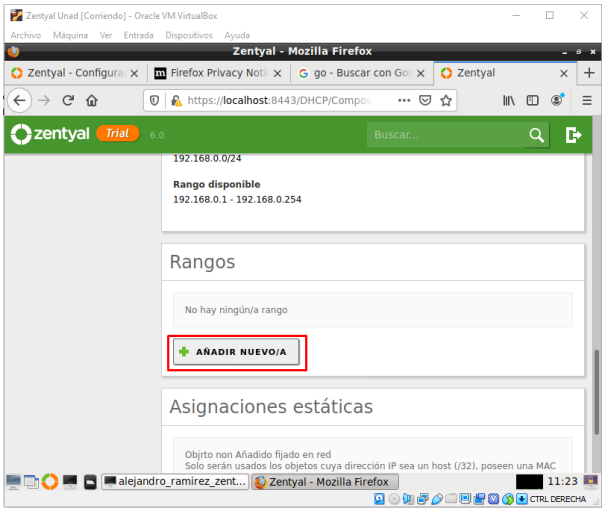
La razón principal por la que se necesita DHCP es para simplificar la administración de las direcciones IP en las redes. No hay dos hosts que puedan tener la misma dirección IP, y configurarlos manualmente puede generar errores. Incluso en redes pequeñas la asignación manual de direcciones IP puede ser confusa, especialmente con dispositivos móviles que requieren direcciones IP de forma no permanente. Además, la mayoría de los usuarios no son lo suficientemente competentes técnicamente para ubicar la información de la dirección IP en una computadora y asignarla. La automatización de este proceso hace la vida más fácil para los usuarios y el administrador de la red.

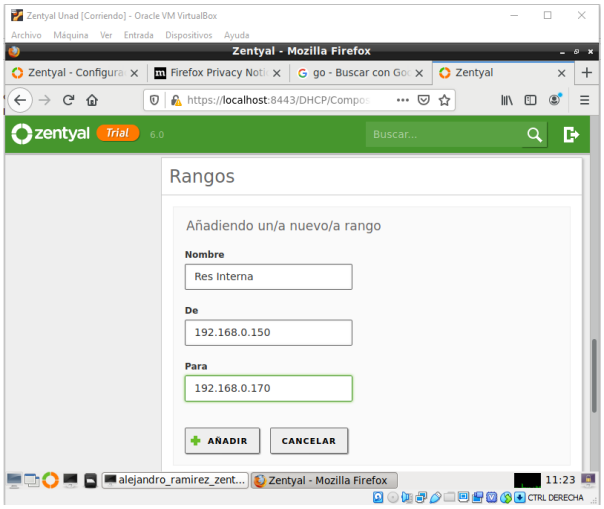
Configuración DHCP

Activación de módulo DHCP

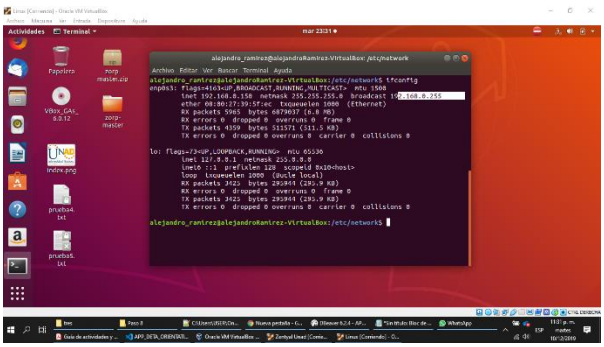


Configuraciones de rango de IPs

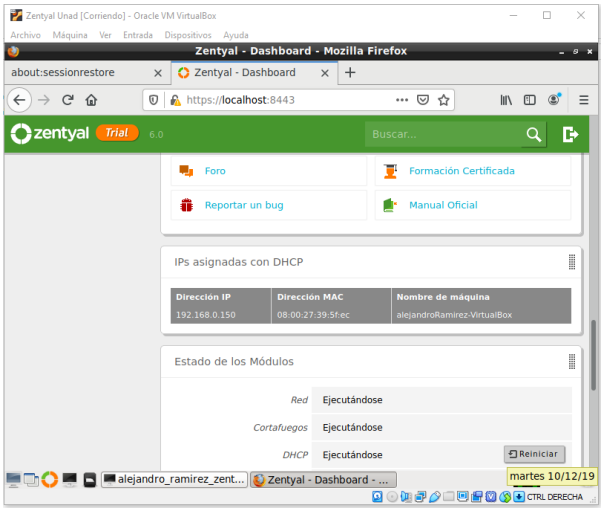




Validación desde el cliente



Validación desde el Zentyal.

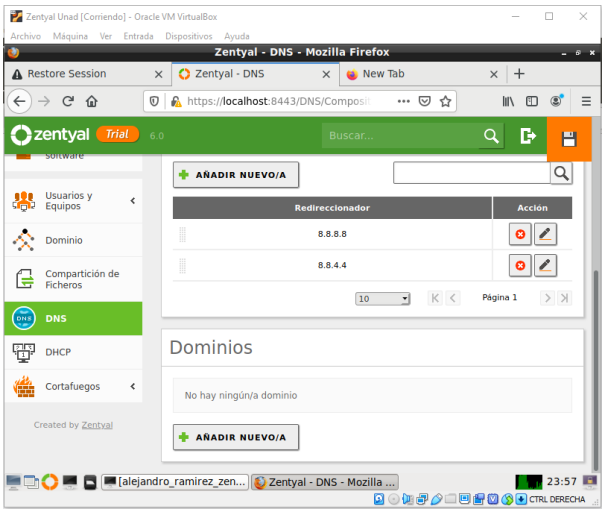


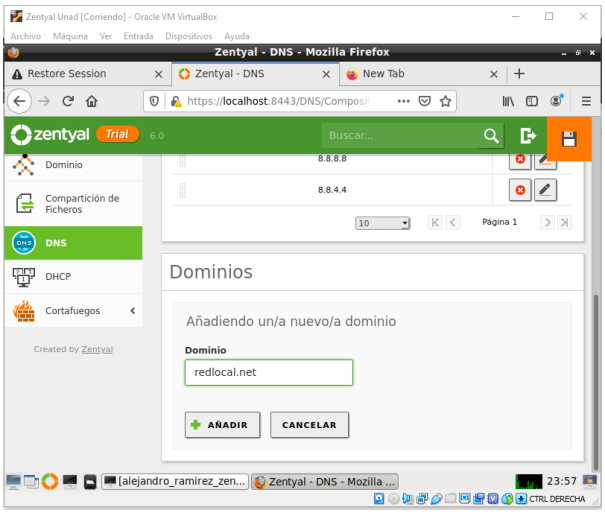
DNS

El Sistema de Nombres de Dominio o DNS es un sistema de nomenclatura jerárquico que se ocupa de la administración del espacio de nombres de dominio (Domain Name Space). Su labor primordial consiste en resolver las peticiones de asignación de nombres. Esta función se podría explicar mediante una comparación con un servicio telefónico de información que dispone de datos de contacto actuales y los facilita cuando alguien los solicita. Para ello, el sistema de nombres de dominio recurre a una red global de servidores DNS, que subdividen el espacio de nombres en zonas administradas de forma independiente las unas de las otras. Esto permite la gestión descentralizada de la información de los dominios.

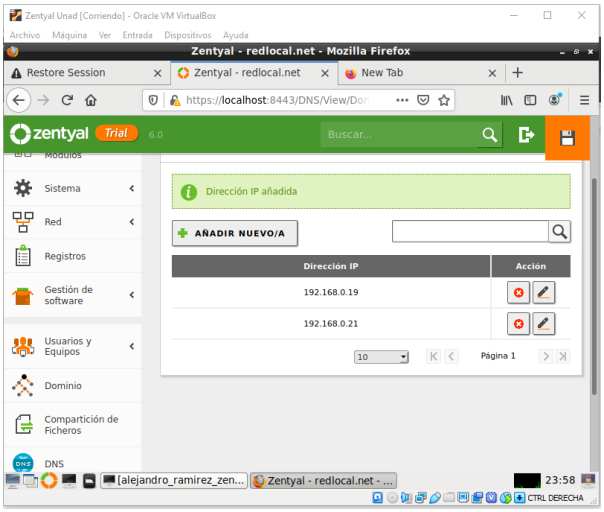
Configuración DNS

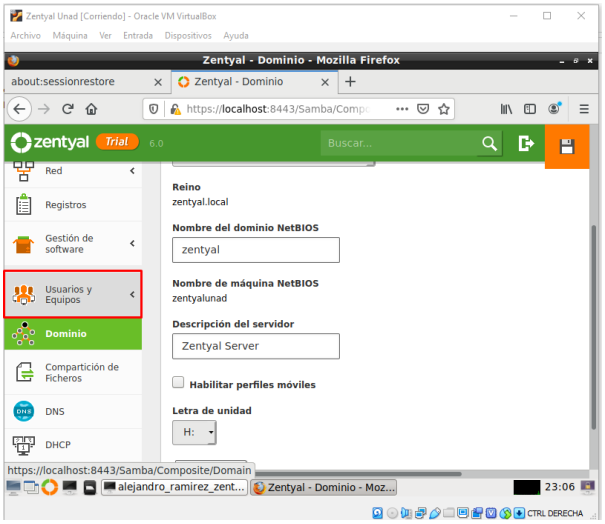
Se configura el módulo de DNS, para ello se agregan las respectivas IPs y se crean el dominio.



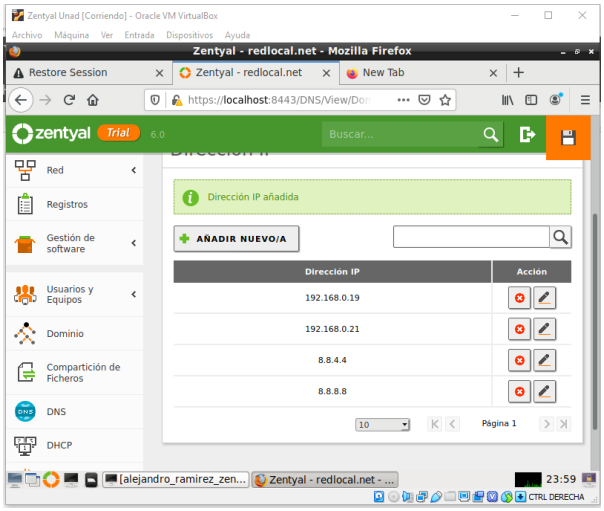


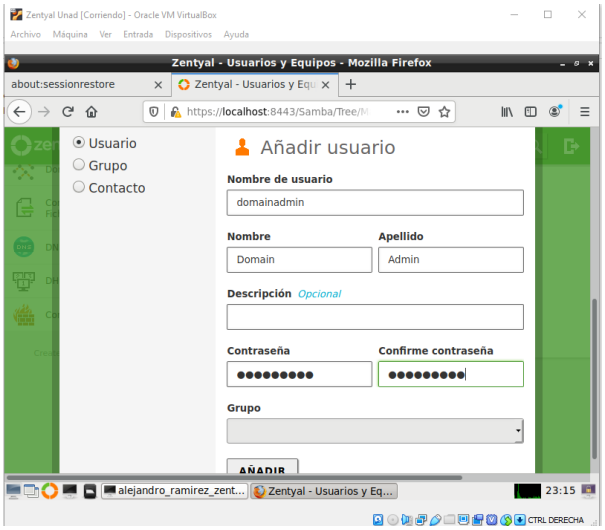
Verificación de IPS.



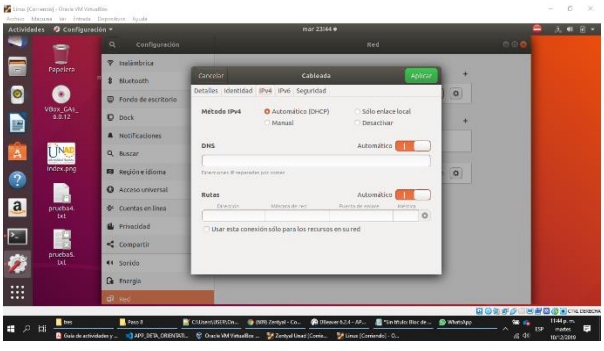


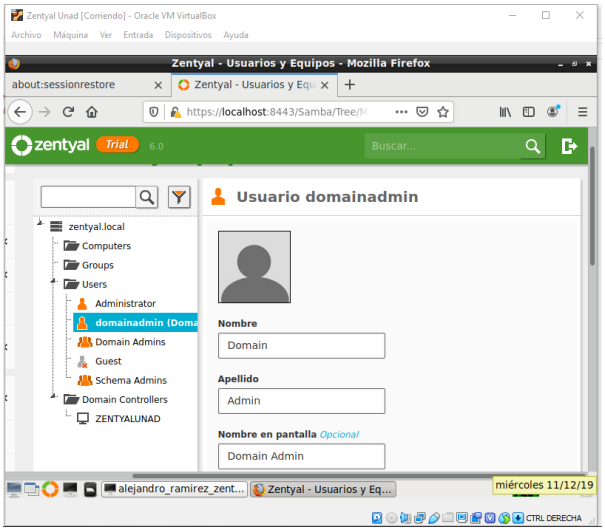
Se añaden los DNS.





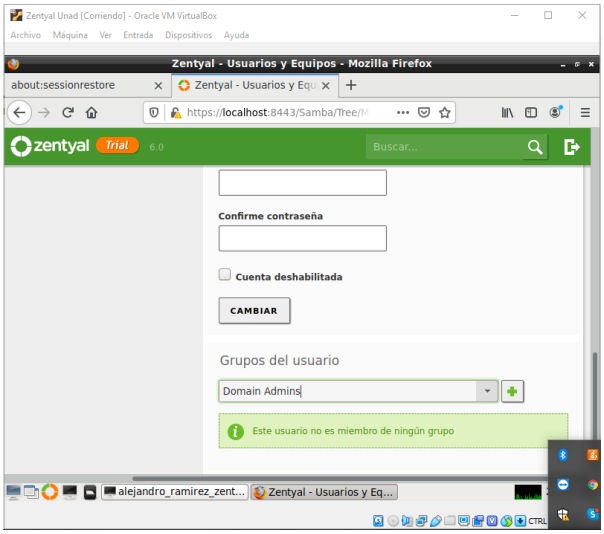
Validación configuración cliente Ubuntu Desktop.



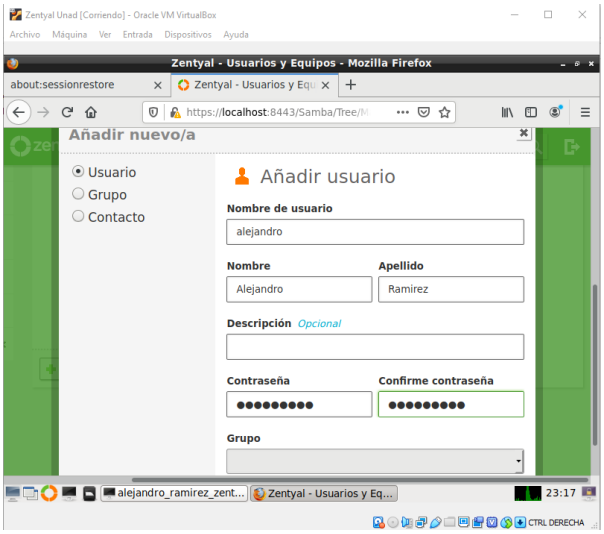


Configuración controladora de dominio

Se crean los usuarios de dominio



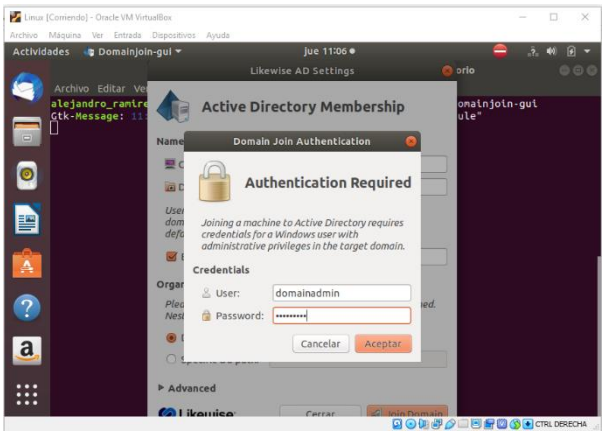
Finalmente creamos un usuario del sistema.



En la máquina de Ubuntu Desktop se deberán de instalar los siguientes paquetes para poder enlazar dicha maquina aun dominio.

- libglade2-0_2.6.4-1ubuntu1.1_amd64.deb
- likewise-open_6.1.0.406-0ubuntu10_amd64.deb
- likewise-open-gui_6.1.0.406-0ubuntu5.1_amd64.deb

realizamos la conexión desde cliente hacia nuestro servidor de dominio



3.3 TEMATICA 2 PROXY NO TRANSPARENTE

Que es un Proxy

Es un servidor (ya sea un programa o dispositivo), que hace de intermediario en las peticiones de recursos que realiza un cliente origen a otro servidor destino; así entonces permite la administración de los accesos de dichos clientes, de la red interna, a otras redes y a Internet.

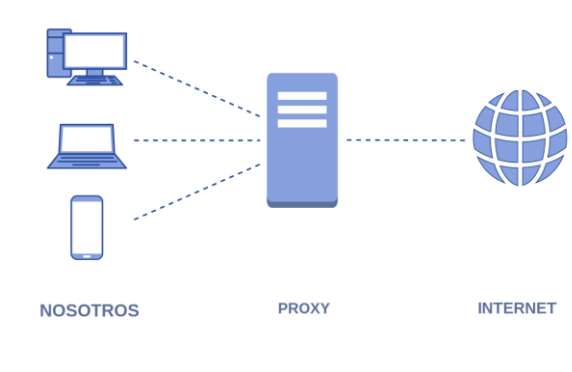


Fig. # Funcionalidad de un Proxy

Características

Se tienen dos tipos de configuración Proxy, el No Transparente y el Transparente, los cuales se caracterizan por:

- El No transparente requiere la configuración en cada cliente (en el aplicativo del usuario normalmente un navegador) de la IP y Puerto del servidor Proxy para permitir la navegación.
- El transparente, no es necesario configurar en los clientes los datos del servicio Proxy para permitir la navegación, dado que se asigna a través de la arquitectura de seguridad.

Ventajas

1) Control; Se puede limitar permisos a los usuarios y dejar solo el permiso del proxy.

2) Velocidad: Si varios usuarios van a pedir el mismo recurso, el Proxy puede realizar un guardado de cache y así no se tiene que contactar de nuevo con el destino.

3) Filtrado: El proxy puede negar algunas peticiones si valida que está prohibido.

Configuración

Podemos evaluar si el Proxy tiene una configuración Trasparente o por el contrario hay que realizar una configuración Manual, en este caso utilizamos la configuración del Proxy No Transparente o Central, el cual solo acepta conexiones provenientes de interfaz de internet interna, por lo cual requiere usar una dirección interna en la configuración del Navegador.

Configuración del S.O. Zentyal Server

Realizada la instalación base del S.O. Zentyal Server, se procede a la ***instalación del paquete HTTP Proxy*** el cual permitirá la administración de los accesos permitidos de los clientes hacia Internet.

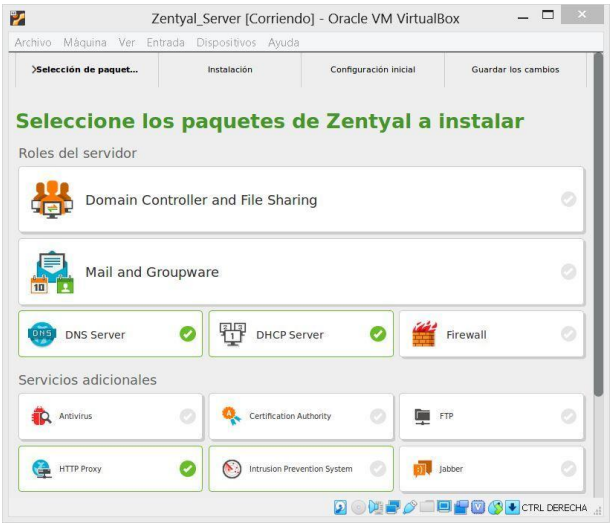


Fig. 17 Selección de Paquete HTTP Proxy

Ahora procedemos a realizar la ***Configuración de las dos interfaces de red*** que tiene la máquina para permitir la funcionalidad del Proxy. La interfaz eth0 se configura como Estática con IP fija interna (ejemplo 192.168.0.10) y la interfaz eth1 se configura como tipo DHCP con IP externa.

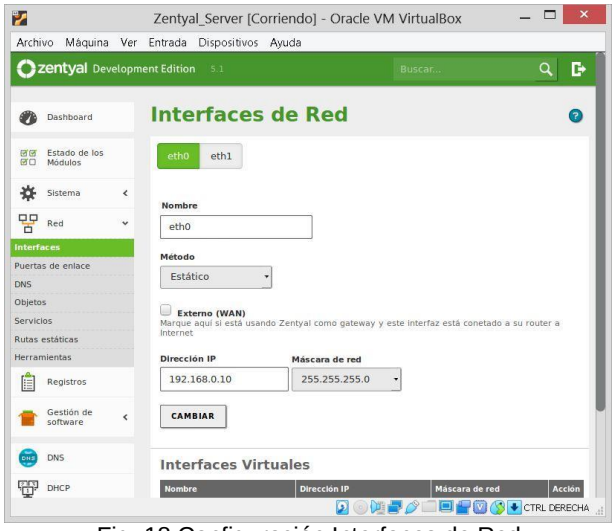


Fig. 18 Configuración Interfaces de Red

Configuración del servicio Proxy No Transparente, para ello entramos en el módulo Proxy HTTP, en Configuración General y nos aseguramos de No dejar seleccionado el Cheek box “Proxy Transparente” y definir el puerto de servicio 3128.

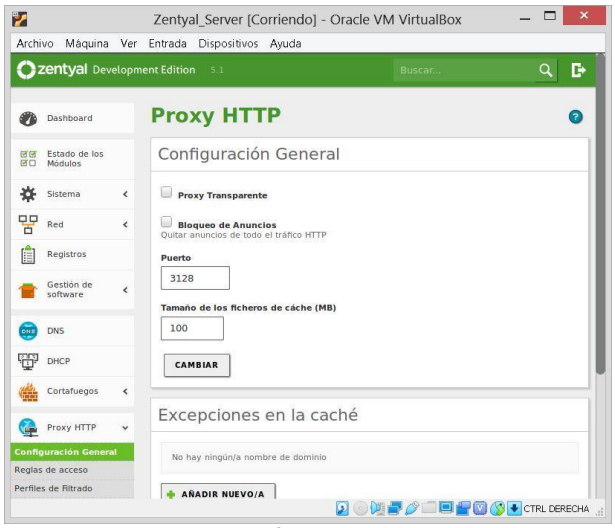


Fig. 19 Configuración Proxy No Transparente

Configuración de Reglas de Acceso asociadas al Proxy No Transparente: Con ayuda de las opciones Reglas de acceso (del módulo de Proxy HTTP) y Objetos (del módulo de Red) Creamos la Lista de objetos “Clientes Autorizados”, la cual contendrá las IPs autorizadas para el acceso a la navegación en Internet a través del Proxy.

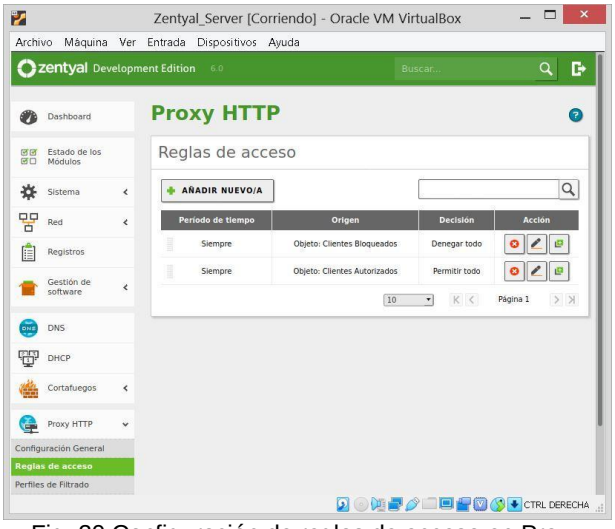


Fig. 20 Configuración de reglas de acceso en Proxy

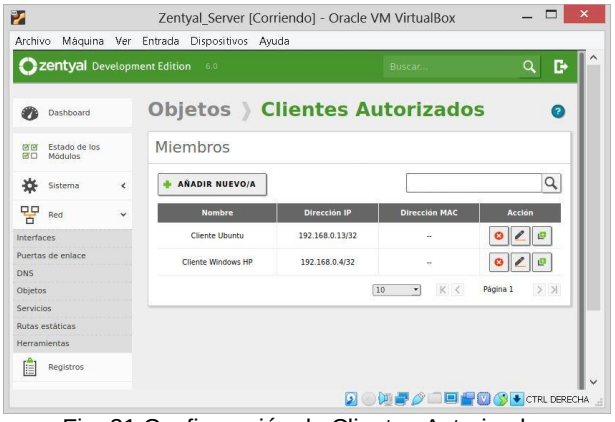


Fig. 21 Configuración de Clientes Autorizados

Validación en el Cliente Ubuntu Desktop del acceso a Internet pasando por el Proxy: Finalmente realizamos la configuración en el navegador del Cliente Ubuntu Desktop para obtener acceso a Internet a través del Proxy preliminarmente configurado y habilitado. En la sección proxy del navegador fijamos la IP y puerto de nuestro servicio Proxy instalado en Zentyal Server.

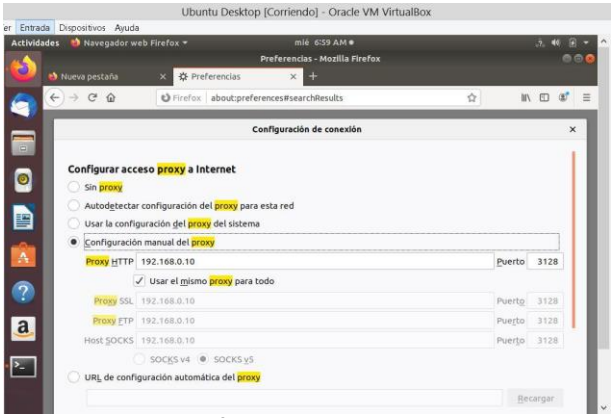


Fig. 22 Configuración Proxy en Cliente Ubuntu Desktop

Verificamos en el Cliente Ubuntu Desktop que la navegación en Internet funcione correctamente, ahora pasando por el Proxy que se ha implementado.

Fig. 23 Prueba de navegación en Cliente Ubuntu Desktop

También certificamos la funcionalidad del control de acceso con el Proxy, realizando un cambio en la configuración de la Lista de Clientes Autorizados; borramos la IP del Cliente Ubuntu Desktop (que para el ejemplo maneja la IP 192.168.0.13).

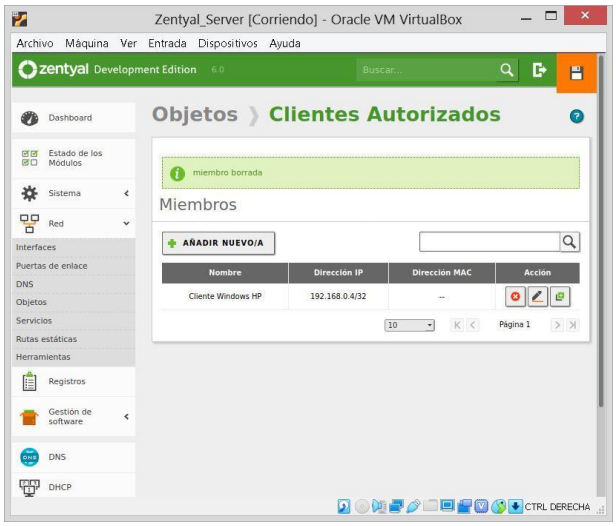


Fig. 24 Borrado de IP Cliente autorizado

Después de grabar el cambio realizado en la Lista de Clientes Autorizados, volvemos a probar en el navegador del Cliente Ubuntu Desktop el acceso a Internet. Observamos que ahora nos aparece un mensaje que indica que el servidor Proxy implementado está ejerciendo el control de acceso y deniega la conexión al Cliente que ya no está incluido en la Lista de autorizados para navegar por Internet.

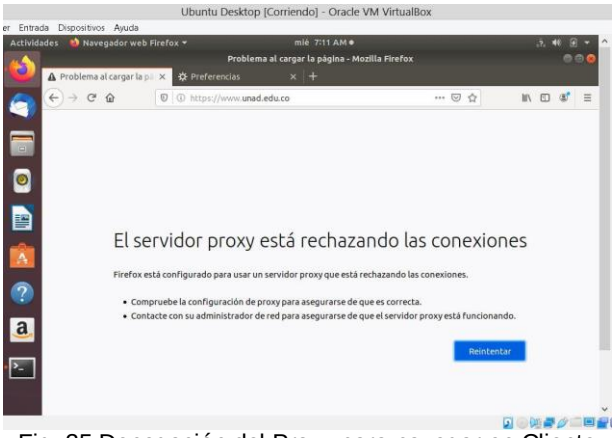
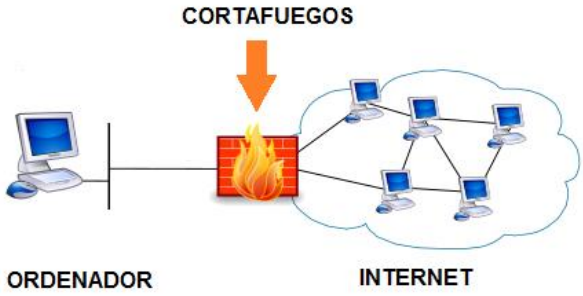


Fig. 25 Denegación del Proxy para navegar en Cliente

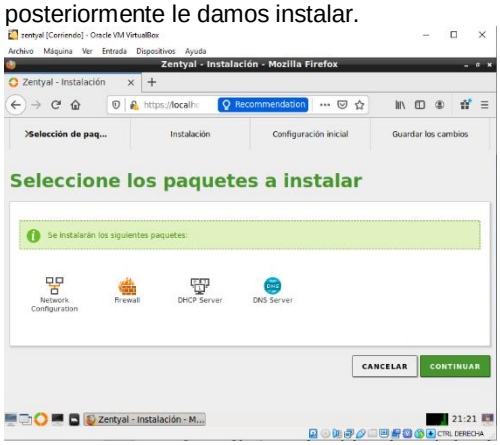
3.4 TEMATICA 3 CORTAFUEGOS



Un cortafuegos o firewall es un sistema que previene el uso y el acceso desautorizados a tu ordenador. Los cortafuegos pueden ser software, hardware, o una combinación de ambos. Se utilizan con frecuencia para evitar que los usuarios desautorizados de Internet tengan acceso a las redes privadas conectadas con Internet, especialmente intranets. [2]

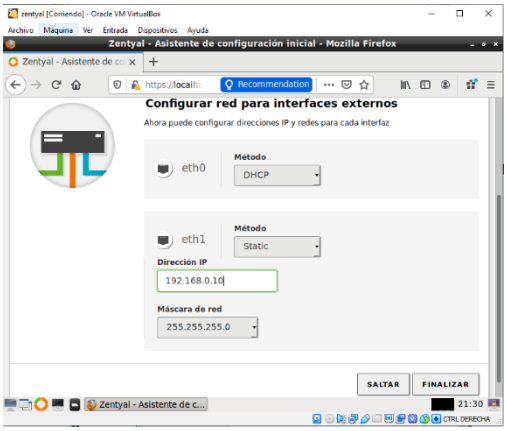
Para instalar y configurar un cortafuego en zentyal server se deben tener en cuenta los siguientes pasos:

- Al iniciar zentyal server por primera vez debemos elegir los servicios requeridos, buscamos la opción cortafuego y posteriormente le damos instalar.

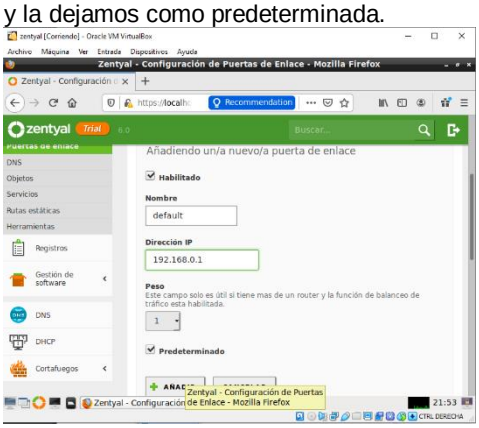


- Luego nos mostrara una ventana donde debemos configurar las dos interfaces de red que creamos, eth0 la dejamos como red externa y eth1 como interna ya que ahí es donde configuraremos el tráfico.

- Para la red eth0 debemos elegir el método DHCP mientras que para la red eth1 seleccionamos el método estático y le asignamos una ip para la interfaz, en este caso 192.168.0.10 y con mascara de red 255.255.255.0.

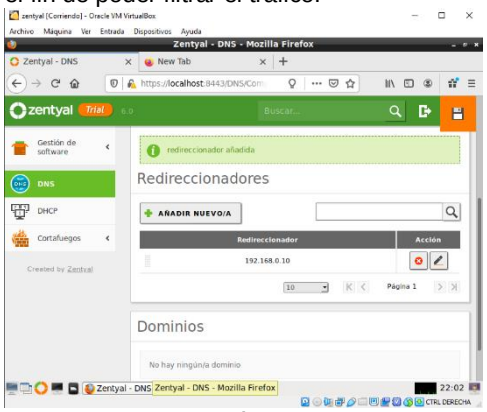


- En las configuraciones del cortafuego debemos dirigirnos a configurar las puertas de enlace, esto con el fin de asignarle una ip a la interfaz, en este caso la 192.168.0.1 y la dejamos como predeterminada.

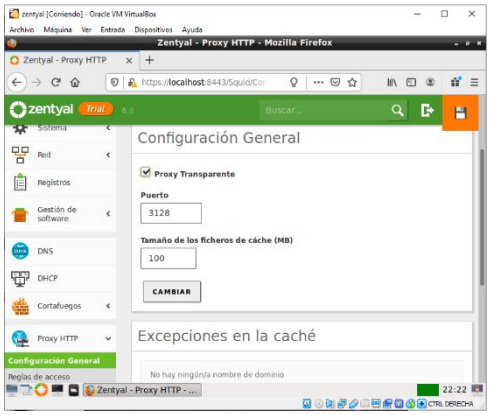


- Nos dirigimos a la parte de DNS y esto con el fin de configurar un direccionamiento, esto quiere decir que todas las peticiones

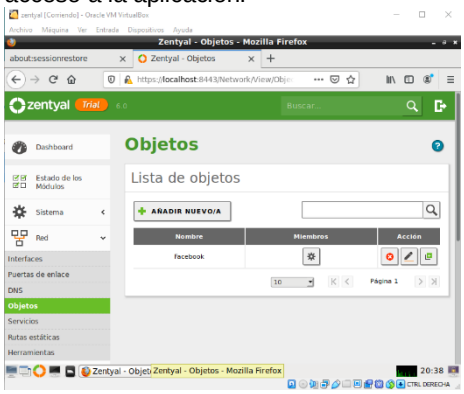
que se realicen dentro de la red local pasan por la puerta de enlace definida y esto con el fin de poder filtrar el tráfico.



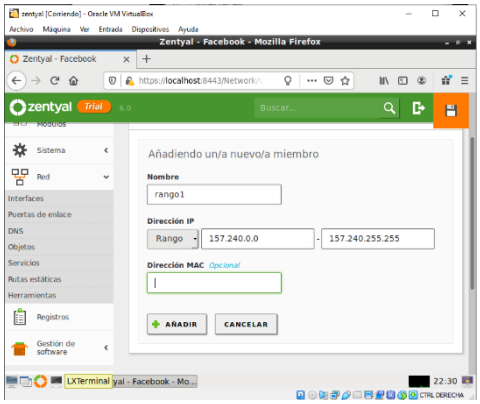
- Nos dirigimos al menú lateral y buscamos la opción proxy para seleccionar proxy transparente y esto con el fin de configurar el tamaño de los ficheros que viajan por la red.



- Nos dirigimos al menú lateral y seleccionamos dentro de la red la opción objetos para crear un objeto llamado Facebook, esto con el fin de conocer que ese grupo se configura para bloquear el acceso a la aplicación.

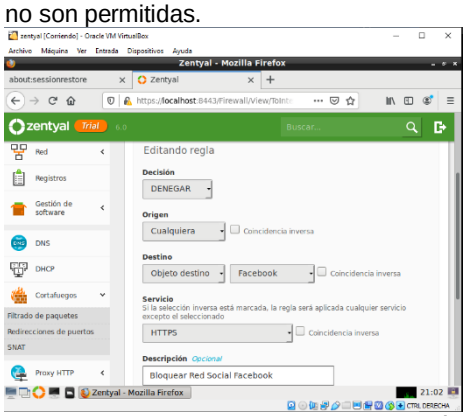


- Luego de tener creado el objeto debemos asignarle miembros, estos miembros son la ip o el rango de ips que se van a bloquear, para este caso 157.240.0 a 157.240.255.255 para que bloque todas las direcciones donde se encuentra alojado el dominio Facebook.com



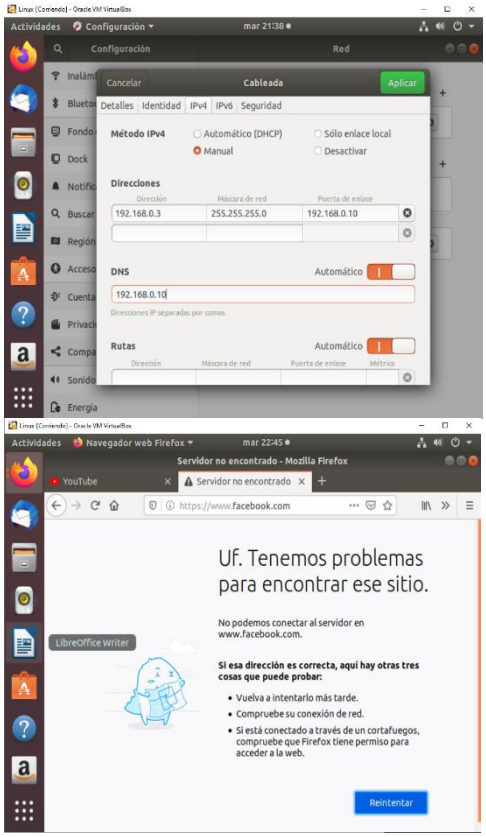
- Nos dirigimos al panel izquierdo y seleccionamos en la parte de cortafuego la opción filtrado de paquetes, posteriormente seleccionamos Reglas de filtrado para las redes internas y configurar reglas

- Seleccionamos añadir nueva regla y nos mostrara ciertas opciones donde nos da la opción tanto como permitir como denegar el acceso, en decisión seleccionamos bloquear, en origen cualquiera y en destino seleccionamos objeto destino y seleccionamos Facebook que creamos con antelación donde se encuentras las ips que no son permitidas.



- Guardamos los cambios y ya quedaría configurado el bloqueo a la red social.
- Nos dirigimos a la máquina virtual que tiene configurado Linux Ubuntu y nos dirigimos a red cableada y configuramos de manera manual la ip y el DNS para que el tráfico lo

filtre el servicio que se acabó de configurar de la siguiente manera. Dirección ip: 192.168.0.3, mascara de red: 255.255.255.0, puerta de enlace: 192.168.0.10 y por último el DNS con dirección 192.168.0.10



3.5 TEMÁTICA 4 FILE SERVER Y PRINT SERVER

zentyal usa samba para implementar SMB/CIFS y gestionar el dominio, Kerberos para los servicios de autenticación. Un servidor de archivos e impresión es el término genérico para cualquier computadora en general este servicio funciona desde una computadora en una red LAN que será designado como servidor de archivos e impresión, con la característica de tener carpetas compartidas para las máquinas que entren dentro de la misma red y una impresora configurada y lista para prestar el servicio a cualquier usuario conectado.

Estos servidores se utilizan para centralizar los archivos de una compañía en una ubicación específica lo que por consiguiente debe estar de forma segura y con los permisos asignados según el rol de cada usuario es decir que puedan o no acceder a ellos o llegar a modificarlos. Los volúmenes del servidor deben estar bajo formato NTFS para lograr asignar permisos en ficheros y el sistema de cifrado de archivos EFS.

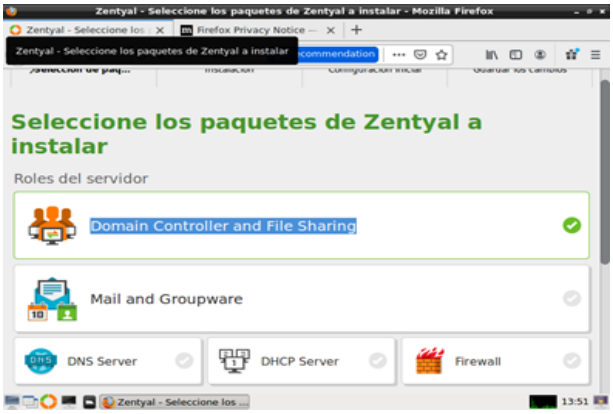


Fig. 38 Habilitación servicio de archivos

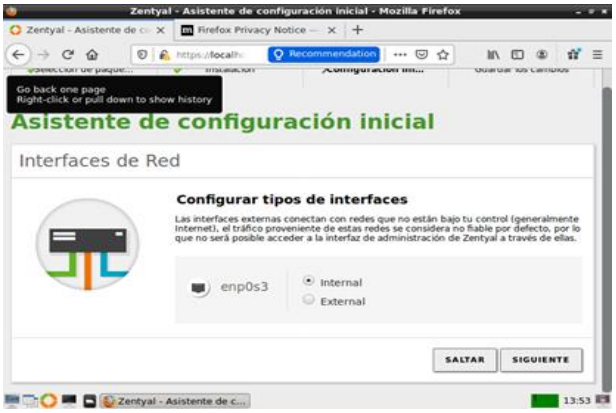


Fig. 39 Configuración de red

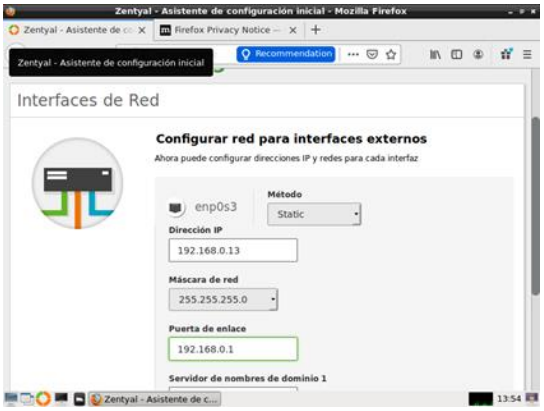


Fig. 40 Definición IP estática

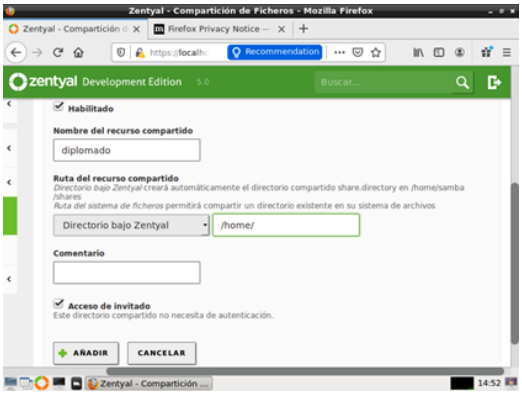


Fig. 41 Configuración de ruta compartida

Servidor de Impresión

el componente SAMBA implementado en ZENTYAL es precisamente para configurar el uso de impresoras compartidas ya sea local o por medio de la red. se organiza para que cualquier cliente de la red local pueda acceder a este recurso sin la necesidad de realizar autenticación

Modos de seguridad en SAMBA.

podemos encontrar dos niveles de seguridad disponibles en el protocolo de red common internet File System que son user-level que es a nivel de usuario y share-level al nivel de recurso, podemos encontrar cuatro formas de realizar esta implementación de seguridad:

Security = user: requiere que los clientes proporcionen un nombre de usuario y una contraseña para conectarse a las acciones. Las cuentas de usuario de Samba son independientes de las cuentas de sistema, pero el paquete libpam-winbind sincronizará los usuarios del sistema y las contraseñas con la base de datos de usuarios de Samba

Security = domain: este modo permite que el servidor Samba se muestre a los clientes Windows como un controlador primario de dominio (Primary Domain Controller, PDC), un controlador secundario de dominio (Backup Domain Controller, BDC) o un servidor de miembros de dominio (Domain Member Server, DMS). Consulte As a Domain Controller para más información.

Security = ADS: permite que el servidor Samba pueda unirse a un dominio de Active Directory como si fuera un miembro nativo. Consulte Active Directory Integration para más información.

Security = server: este modo se usaba antes de que Samba pudiera ser un servidor de miembros, pero ahora no debería usarse debido a ciertos problemas de seguridad. Consulte la sección sobre seguridad del servidor en la guía de Samba para más información.

Security = share: permite que los clientes puedan conectarse a los recursos compartidos sin necesidad de proporcionar un nombre de usuario y una contraseña

El modo de seguridad que vaya a elegir dependerá de su entorno y de lo que necesite que haga su servidor Samba.

Ventajas

Ahorro de espacio: Ya no es necesario comprar una impresora dedicada para cada usuario, por lo tanto, usted puede ahorrar el espacio, la electricidad y los costes de mantenimiento.

Instalación rápida: Agregar una impresora a la red en cuestión de minutos. No hay necesidad de cerrar su red.

Velocidad y Flexibilidad: Una impresora de red por lo general funciona más rápido que las impresoras láser o de inyección que no tienen la capacidad de ser conectadas a la red.

Algunas impresoras multifunción pueden enviar faxes, imprimir documentos, imágenes de escaneo y copia, al momento.

La flexibilidad, evitando colas o retrasos: Redes más de una o todas las impresoras pueden ofrecer una gran flexibilidad.

Desventajas

Altos costos: La cantidad de potencia necesaria para mantener la máquina en funcionamiento es alto al igual que la cantidad de tinta.

Mantenimiento: Puede ser un problema para las empresas que tienen una gran cantidad de impresión,fax y necesidades de copiado.

Tiempo: Algunas personas pueden tener que esperar para usar la máquina, deteniendo su tiempo de producción.

3.6 TEMATICA 5 VPN

VPN (Virtual Prívate Network) es una tecnología de red privada que nos permite conectar una o más computadoras para trabajar desde casa o desde otro lugar fuera de la empresa y accediendo a los recursos compartidos.

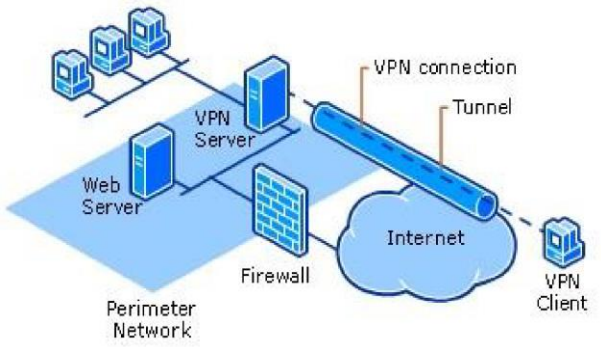


Fig. 42 esquema configuración VPN

Se debe tener en cuenta que no todos los usuarios tienen el privilegio de acceso a la VPN, son personas seleccionadas de acuerdo al cargo y responsabilidades que tienen. Por seguridad de la información, se tiene en cuenta los siguientes protocolos: IPsec (Internet Protocolo Security): permite mejorar la seguridad a través de algoritmos de cifrado robustos y un sistema de autentificación más exhaustivo. IPsec posee dos métodos de encriptado, modo transporte y modo túnel. Así mismo, soporta encriptado de 56 bit y 168 bit (triple DES). PPTP/MPPE: tecnología desarrollada por un consorcio formado por varias empresas. PPTP soporta varios protocolos VPN con cifrado de 40 bit y 128 bit utilizando el protocolo Microsoft Point to Point Encryption (MPPE). PPTP por sí solo no cifra la información.

L2TP/IPsec (L2TP sobre IPsec): tecnología capaz de proveer el nivel de protección de IPsec sobre el protocolo de túnel L2TP. Al igual que PPTP, L2TP no cifra la información por sí mismo.

Una de las grandes ventajas que tiene esta tecnología es que nos permite ingresar desde cualquier lugar a los servidores donde se encuentre configurado el servicio sin ninguna restricción geográfica.

Procedimiento de configuración

Al momento de la configuración inicial de Zentyal debemos seleccionar el módulo de VPN para que nos permita realizar la posterior configuración de este.

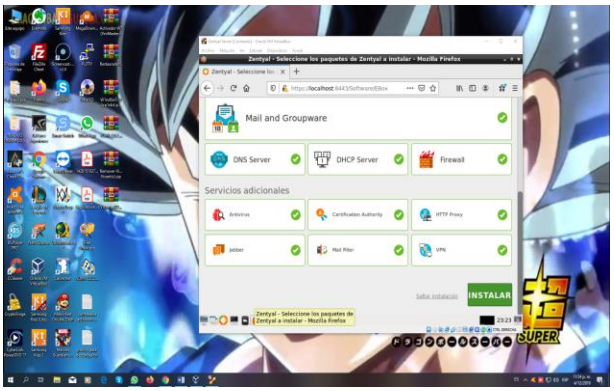


Fig. 43 Selección módulo VPN

Luego de realizar las configuraciones iniciales necesarias en el Zentyal este nos muestra una dashboard donde se encuentra el módulo VPN

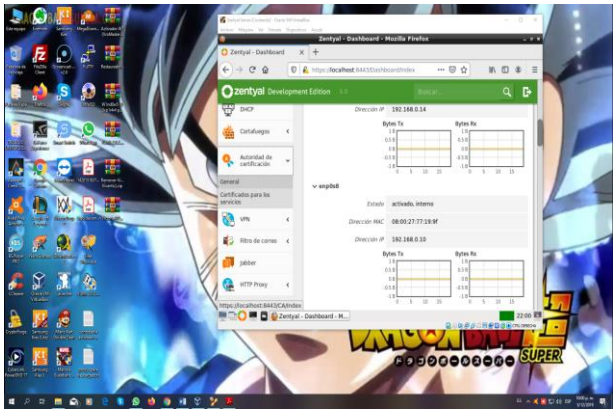


Fig. 44 Modulo VPN

Como primer paso debemos crear la certificación para el servidor (Zentyal Server) la cual generamos desde el módulo de autoridad de certificación, llenamos los datos y damos clic en crear.

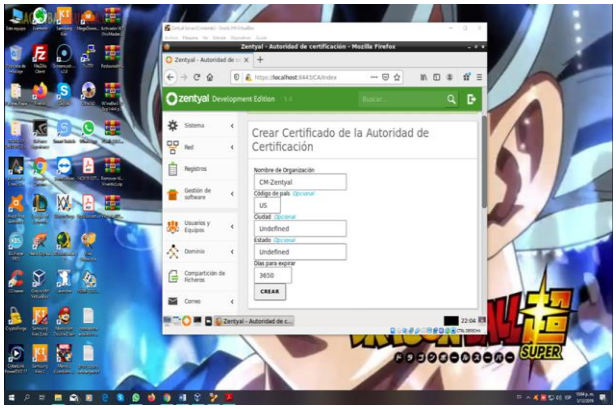


Fig. 45 Certificado servidor Zentyal

Segundo paso vamos al módulo VPN y damos clic en servidores, llenamos los datos y finalizamos dando clic en añadir.

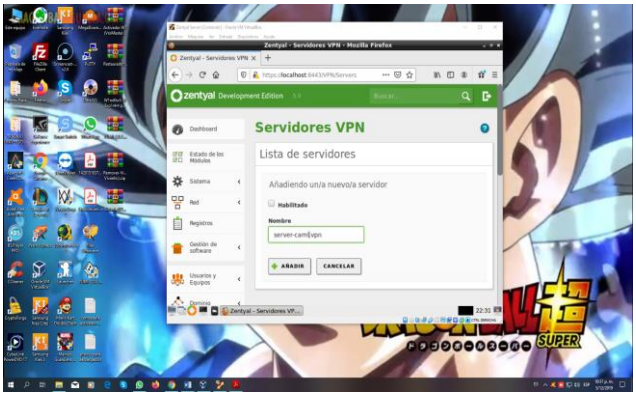


Fig. 46 Creación de servidor VPN

Tercer paso regresamos nuevamente al módulo de autoridad de certificación para crear el certificado del servidor VPN, llenamos los datos y damos clic en expedir.

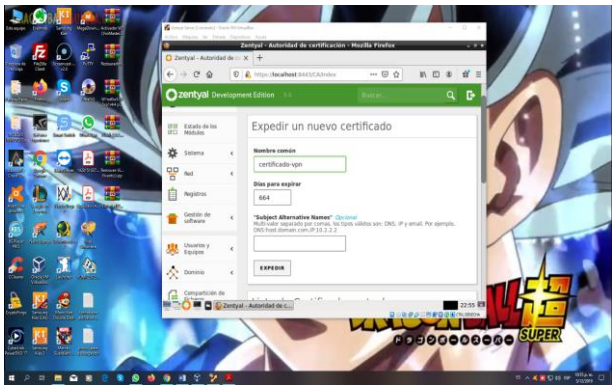


Fig. 47 Certificado servidor VPN

Cuarto paso regresamos nuevamente al módulo VPN y configuramos el servidor creado, la cual en certificado de servidor elegimos el que le creamos a la VPN, dejamos por defecto las demás configuraciones y seleccionamos la interfaz TUN

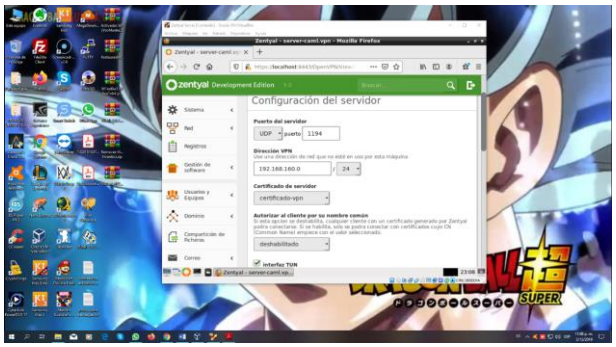


Fig. 48 Configuración del servidor VPN

Quinto paso en este mismo modulo vamos a descargar los paquetes de configuración de cliente tanto para Windows como para Linux, el procedimiento es elegir el tipo de cliente si elegimos Windows él nos da la opción de descargar también el instalador de la aplicación OpenVPN e ingresamos la dirección del servidor para que pueda acceder el cliente.

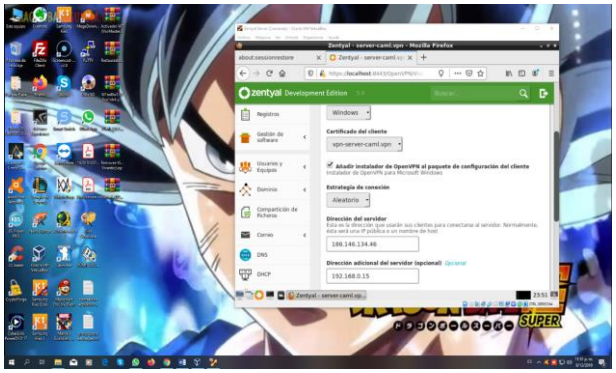


Fig. 49 Descargue de paquetes cliente Windows

Sexto paso, cuando generamos el paquete este nos muestra una ventana emergente con el archivo en formato (.Zip) el cual debemos descargar en el equipo cliente.

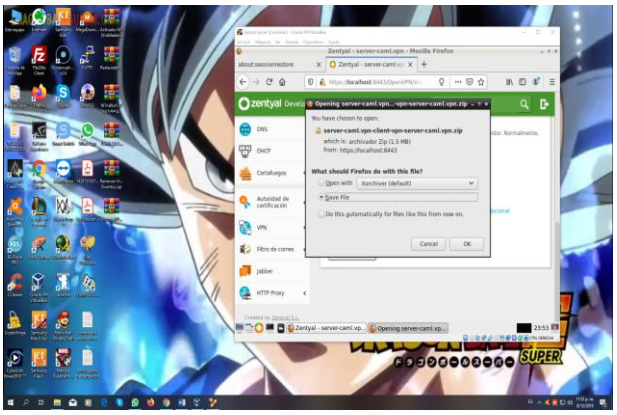
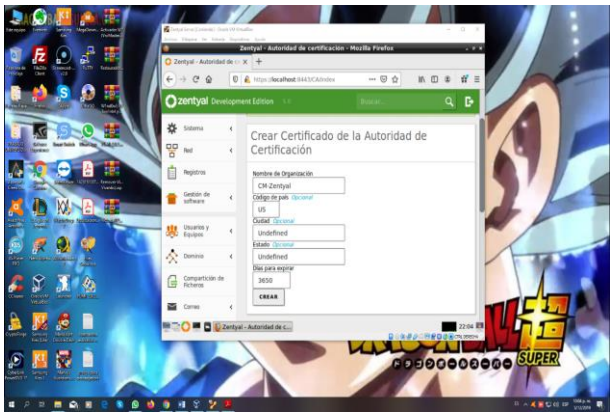


Fig. 50 Paquete instalador cliente Windows

Séptimo paso, ahora hacemos el mismo procedimiento para el cliente Linux, pero en este caso se debe instalar en el equipo cliente por medio de consola el OpenVPN, los demás datos son iguales.



Octavo paso, cuando generamos el paquete este nos muestra una ventana emergente con el archivo en formato (.tar.gz) el cual debemos descargar en el equipo cliente.

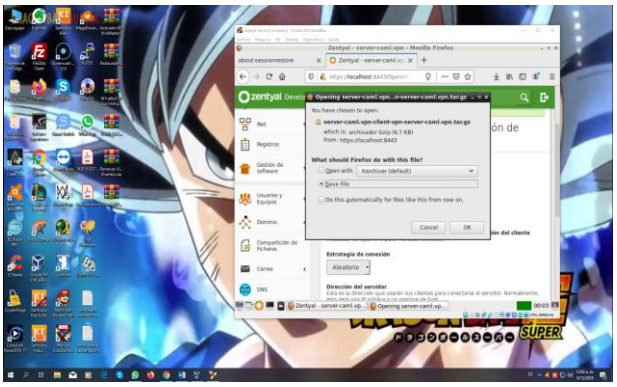


Fig. 51 Paquete instalador cliente Linux

Noveno paso, verificamos en el panel principal de la dashboard si se está ejecutando el servicio de la VPN la cual nos debe aparecer con en la siguiente imagen.

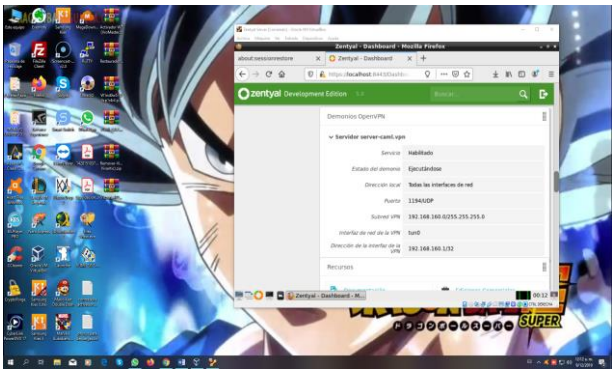


Fig. 52 Verificación de ejecución del servicio VPN

Décimo paso, realizamos la instalación del programa OpenVPN en el cliente Windows para que nos permita realizar la conexión con los archivos generados

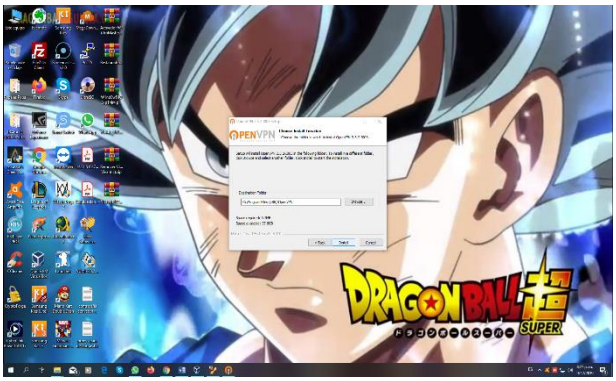


Fig. 53 Instalación OpenVPN en cliente Windows

Décimo primer paso, al finalizar la instalación este nos deja un icono en la parte inferior derecha parecida a la de conexión de internet, pero en este caso con un candado, damos clic derecho en este icono y damos importar

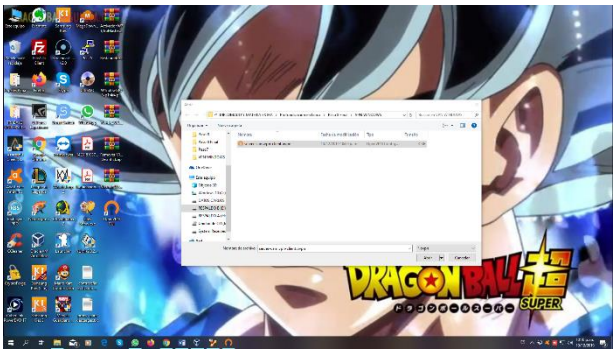


Fig. 54 Importar archivo para conexión VPN

Al realizar el anterior procedimiento finalizamos dando clic en conectar, lo que nos permite la comunicación entre el servidor Zentyal y nuestro equipo cliente Windows a través de la VPN.

Para el cliente Linux en este caso Ubuntu la instalación del OpenVPN se realiza a través de la terminal como se muestra en la siguiente imagen

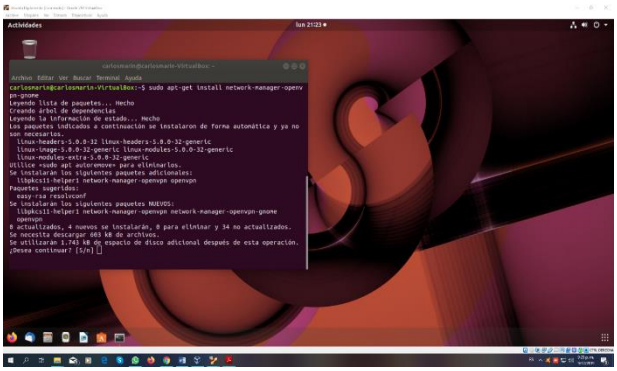


Fig. 55 Instalación OpenVPN en cliente Linux

Al realizar la instalación nos dirigimos a la parte de red y damos clic en añadir VPN, configurándola como se muestra la siguiente imagen

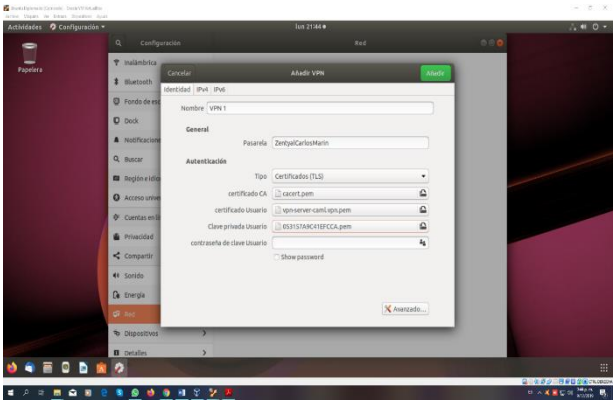


Fig. 56 Configuración VPN en cliente Linux

Finalizamos ingresando a la parte superior derecha donde está el icono de conexiones de red y damos en la opción conectar de la VPN

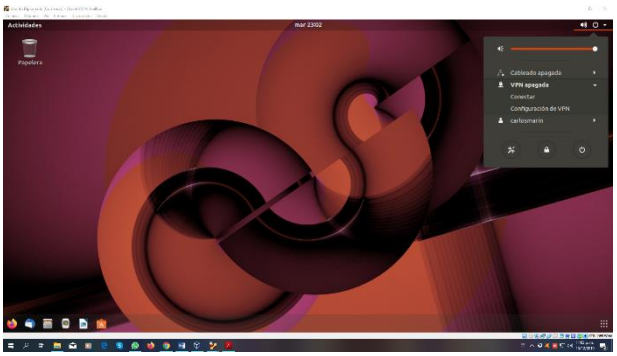


Fig. 57 conexión de la VPN

4 CONCLUSIONES

Al concluir con la actividad se pudo comprender la importancia de conocer los diferentes servidores bajo el sistema operativo Linux como lo es Zentyal Server, posee muchos servicios entre ellos el poder configurar un cortafuego para así filtrar todo el contenido que pasa por la red, esto nos permite tanto autorizar como denegar acceso a url publicadas en internet, nos permite bloquear rangos de direcciones y configurar paquetes para que solo dichas ips dentro de la red posean las reglas de bloqueo o acceso, el único inconveniente es que el servidor tiene licencia comercial por tal tiene un costo por su uso.

5 REFERENCIAS BIBLIOGRÁFICAS

[1] M. Cabrera, «Como instalar Zentyal server paso a paso FÁCIL,» 07 Abril 2018. [En línea]. Available: https://drivemeca.blogspot.com/2018/04/como-instalar-zentyal-server-paso-paso.html. [Último acceso: 04 Diciembre 2019].

[2] Masadelante.com, «¿Que es un Cortafuegos?,» 10 Diciembre 2019. [En línea]. Available: https://www.masadelante.com/faqs/cortafuegos. [Último acceso: 10 Diciembre 2019].

[3] Doc.zentyal.org, «Cortafuegos,» 05 Diciembre 2019. [En línea]. Available: https://doc.zentyal.org/es/firewall.html. [Último acceso: 05 Diciembre 2019].

[4] Whois.domaintools.com, «Whois Lookup,» 06 Diciembre 2019. [En línea]. Available: http://whois.domaintools.com/. [Último acceso: 06 Diciembre 2019].

[5] Es/3.5/Servicio de redes privadas virtuales (VPN) con OpenVPN - Zentyal Linux Small Business Server. (n.d.). Retrieved May 15, 2018, from https://wiki.zentyal.org/wiki/Es/3.5/Servicio_de_redes_privadas_virtuales_(VPN)_con_OpenVPN

[6] Configuración y conexión a un servidor VPN con Zentyal usando OpenVPN. (2015). Retrieved from https://www.youtube.com/watch?v=3rNfipxE-9o

[7] Meseguer, M. (2013, June 18). Instalar y configurar el cliente OpenVPN en GNU/Linux » Sobrebits. Retrieved May 16, 2018, from https://sobrebits.com/instalar-y-configurar-cliente-openvpn-en -gnulinux/