Debatir, generar, determinar e implementar soluciones gnu/linux

Blanca Lucia Castaño Marín - Cód.: 44.002.320
E-mail: castamar123@gmail.com
Gerardo Ramos Jara - Cód.: 1.117.531.028
E-mail: geramos323@gmail.com
Luis Fernando Molina – Cód.: 17.647.761
E-mail: moliferc@gmail.com
Christian Ricardo Almanza Castañeda - Cód: 1.122.136.507
E-mail:crac_0709@hotmail.com
Ángela María Mejía Gaez - Cód: 1.062.296.454
E-mail: angelamejiagaez@gmail.com

***Resumen*— Este artículo describe los usos de los firewalls y soluciones a través de una implementación y una configuración detallada para bloquear el acceso a los sitios web de entretenimiento y las redes sociales, al enumerar las reglas y políticas que se crearon. Por un lado, Zentyal proporciona administración de servidores, incluida la funcionalidad de firewall entre muchos otros, configurable a través del acceso a la interfaz web. Este artículo tiene como objetivo describir las ventajas de implementar firewalls en grandes empresas como La Aeronáutica Civil de Colombia.**

***Palabras claves:* Zentyal Server, Cortafuegos, Sitios Web de entretenimiento, Redes Sociales, Restricción, Políticas de acceso, Reglas de Cifrado.**

I. Introducción

En la actualidad, las compañías disponen de sus propiosservidores, estaciones de trabajo y dispositivos móviles que generalmente están interconectados, que aunque facilitan muchas tareas,también introducen ciertos riesgos.

Hoy en día todas las pequeñas y medianas empresas requieren soluciones de servidores locales; muchas de las cuales disponen de sus propios servidores, estaciones de trabajo y dispositivos móviles que generalmente están interconectados, que aunque facilita muchas tareas, también introduce ciertos riesgos. Para suplir la necesidad de tener toda una red y tener controlados y monitoreados a todos los usuarios de un intranetes necesario tener una herramienta que sea capaz de controlar todo el intercambio de datos.

Para el desarrollo de esta etapa final de Diplomado de profundización en Linux, se implementó la distribución de Linux, Zentyal 5.01 que ofrece soluciones web.

El desarrollador del Zentyal Linux Small Business Server, nos presenta un servidor Linux que es fácil de usar y que tiene compatibilidad nativa con Microsoft Active Directory®.

El Servidor Zentyal 5.0 se basa en Ubuntu Server 16.04 LTS (XenialXerus) e incluye todas las últimas versiones del software integrado. La principal mejora que introduce este servidor es la integración de la última versión de Samba 4.5.1. Debido al rápido desarrollo del proyecto Samba, desde esta versión en adelante, el Servidor Zentyal integra los últimospaquetes estables de Samba publicados por los desarrolladores de Samba (upstream). Esto permite una introducción más rápida de nuevas características, parches y actualizaciones en el Servidor Zentyal.

Por otro lado, Zentyal contiene módulos de seguridad entre los cuales se encuentran el cortafuego o firewall que es una de las varias formas de proteger una red y de evitar los ataques a las redes, tales como Eavesdropping, PacketSniffing, Snooping, Tampering, Spoofing, Jamming o Flooding, entre otros.En pocas palabras, la razón para la instalación de cortafuegos radica en la protección de una red privada contra intrusos, permitiendo a su vez el acceso autorizado desde y hacia el exterior.

En el caso de la Aeronáutica Civil de Colombia, se hace necesaria la implementación de cortafuegos de sitios web de entretenimiento y redes sociales para evitar el hackeo de información importante en la compañía. Las políticas de acceso de Zentyal están establecidas de forma que la configuración inicial sea lo más estricta posible, para garantizar la seguridad desde el primer momento a través de la configuración de cortafuegos.

El presente artículo describe y evidencia el uso de cortafuegos a través de la 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.

II. Descripción del problema

La Aeronáutica Civil de Colombia, empresa que se encarga del desarrollo ordenado de la aviación civil, de la industria aérea y la utilización segura del espacio aéreo colombiano, facilitando el transporte intermodal y contribuyendo al mejoramiento de la competitividad del país, presenta problemáticas en torno a migración y puesta en marcha de los servicios de gestión enDHCP Server, DNS Server y Controlador de Dominio, Proxy no transparente, Cortafuegos, File Server - Print Server y VPN.De esa manera se requiere la administración y control de una distribución GNU/Linux basada en Ubuntu, pero enfocada a la implementación de servicios de infraestructura IT de mayor nivel para Intranet y Extranet en instituciones complejas como la Aeronáutica Civil. El presente artículo responde a la problemática relacionada con la utilización de cortafuegos a través de la 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.

III. Implementación y puesta en marcha de soluciones para GNU/LINUX.

Marco teórico

Para el desarrollo del proyecto es necesario describir algunos conceptos tales como Zentyal, Cortafuegos, Políticas de Acceso y reglas de filtrado.

*Zentyal*es es considerado una distribución GNU/Linux para gestión de servidores, incluyendola funcionalidad de cortafuegos entre varias otras, configurable mediante acceso por interfaz web. Esta aplicación fue diseñada para su uso en oficinas domésticas y PYMEs.

Un C*ortafuegos* (firewalleninglés) es una parte de un sistema o una red que está diseñada para bloquear el acceso no autorizado, permitiendo al mismo tiempo comunicaciones autorizadas. Es decir, el cortafuegos crea una barrera entre los datos privados de nuestra computadora y las amenazas externas que nos pueden atacar cuando estamos conectados a una red.

Los cortafuegos pueden ser implementados en hardware, software, o una combinación de ambos; Los cortafuegos se utilizan con frecuencia para evitar que los usuarios de Internet no autorizados tengan acceso a redes privadas conectadas a Internet, especialmente intranets. Todos los mensajes que entren o salgan de la intranet pasan a través de los cortafuegos, que examinan cada mensaje y bloquean aquellos que no cumplen los criterios de seguridad especificados.

Existen diferentes tipos de cortafuegos entre los cuales se encuentran:

- *Nivel de aplicación de pasarela*, que aplica mecanismos de seguridad para aplicaciones específicas, tales como servidores FTP y Telnet.
- *Circuito a nivel de pasarela*, que aplica mecanismos de seguridad cuando una conexión TCP o UDP establecida.
- *Cortafuegos de capa de red o de filtrado de paquetes* que funciona a nivel de red (capa 3 del modelo OSI, capa 2 del stack de protocolos TCP/IP) como filtro de paquetes IP.
- *Cortafuegos de capa de aplicación*, que trabaja en el nivel de aplicación (capa 7 del modelo OSI), demanera que los filtrados se pueden adaptar a características propias de los protocolos de este nivel.

Por otro lado, se entienden las *Políticas de acceso* como las estrategias que están establecidas de forma que la configuración inicialsea lo más estricta posible, para garantizar la seguridad desde el primer momento.

La definición de las políticas del cortafuegos se hace desde *Cortafuegos en el filtrado de paquetes*.

Finalmente, las *Reglas de Filtrado* hacen parte de la Política y permiten definir los Servicios de red para especificar a qué protocolos y puertos se aplican las reglas y los Objetos de red para especificar sobre qué direcciones IP de origen o de destino se aplican.

A. Implementación de un Proxy no transparente.

Los servicios de proxy web pueden ser configurados para operar ya sea en modo transparente o no transparente, siendo estos muy diferentes debido a las características que cada uno de estos posee; y aunque son muy diferentes, los dos pueden ser utilizados al mismo tiempo, por lo que el habilitar el proxy no transparente, no hará que deje de funcionar el proxy no transparente.

El uso del proxy transparente requiere una estructuración mínima de la red o nula, lo que hace que no se requiera de algún tipo de configuración especial para los clientes, lo que nos brinda la posibilidad de que el servicio de proxy sea activado y desactivado de manera casi inmediata debido a que todo el tráfico que es destinado a internet y llega al puerto 80 se redirige de forma automática a través del proxy.

Por otra parte una de las principales razones para hacer uso del proxy no trasparente, es que tanto el navegador como las aplicaciones utilizadas por el cliente sepan que se está haciendo uso de este tipo de servicio y actué en función de las reglas impuestas por el proxy.

Aunque para muchos el uso del proxy no transparente es

complicado debido a las configuraciones que deben realizarse en los equipos y navegadores de los clientes, en última instancia resulta siendo favorable para estos, además de que suministra un servicio proxy más flexible y potente, hará nuestra red más segura debido a que los spyware y gusanos informáticos que utilizan los servicios web para su propagación, les será difícil acceder a la redporque no conocen la configuración del proxy, lo que reduce el peligro software malicioso en nuestro sistema.

Las configuraciones de proxy apropiadas deben configurarse en los equipos y navegadores de los clientes, lo cual se puede hacer de diferentes maneras:

- Manual: la cual se puede realizar en la mayoría de los navegadores web y aplicaciones como parte de la configuración de las conexiones.
- Script de configuración automática: esto se puede hacer mediante Smoothwall que proporciona unarchivo proxy.pacque, el cual se puede usar para configurar automáticamente un proxy en la mayoría de los navegadores de Internet.
- Dominio de Microsoft Windows: en un dominio de Windows 2000 en adelante, la configuración del proxy se puede configurar en la política de seguridad del dominio.
- Descubrimiento automático: muchos navegadores admiten el descubrimiento automático de la configuración del proxy mediante el protocolo WPAD (Web Proxy Auto-Discovery).
- Uso de DHCP: mediante el uso de DHCP es posible distribuir y establecer la configuración del proxy, siendo este método uno de los preferidos debido a permite un mejor uso políticas de seguridad.
- Script de inicio de sesión de Microsoft Windows: el script de inicio desesión de Windows esusado para importar un archivo de registro el cual configurará automáticamente la configuración del proxy en todo el sistema.
- Archivos .ini: en navegadores como Firefox es posible configurar automáticamente archivos .ini, los cuales se pueden copiar o modificar como parte de la secuencia de comandos de inicio de sesión en una red Microsoft Windows o Linux.
- Aplicaciones deterceros: existen aplicaciones de terceros disponibles para Windows que al iniciar sesión pueden configurar automáticamente servicios de proxy en el navegador web. Estos van desde simples programas diseñados específicamente para automatizar la configuración del proxy, o aplicaciones más sofisticadas que proporcionan una gama de servicios como la supervisión del escritorio de los usuarios.

B. Implementación de un Cortafuegos.

En el caso del proyecto, se utilizará el cortafuegos de capa de aplicación para sitios Web HTTP y HTTPS, proceso que se describe a continuación:

1. *Restricción de la apertura de sitios Web de entretenimiento y redes sociales HTTP*

Para la restricción de sitios Web de entretenimiento y redes sociales HTTP se utilizó le módulo HTTP Proxy. Este módulo ofrece una manera muy sencilla de aplicar filtros por url, por contenido o por extensiones de archivo, de manera que nos puede permitir el acceso a una determinada web pero no poder descargar archivos .zip, o no poder ver clips de videos:

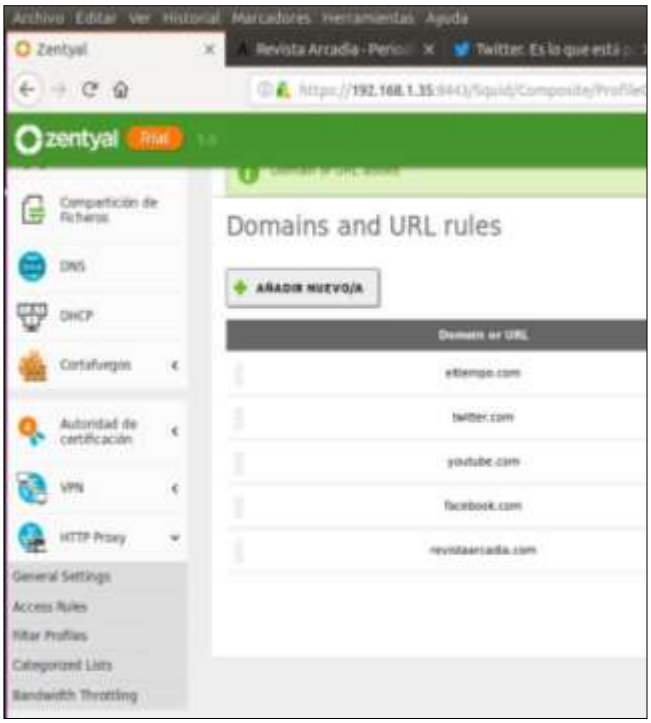

Fig.1 restriccion de sitios web desde zentyal

2. *Configuracion de reglas de filtrado.*

Para la restricción de estos sitios Web, se utilizó el Módulo "Cortafuegos", puesto que aunque los sitios Web HTTP se bloquearon a través las reglas del proxy, estono aplica a páginas https como facebook, gmail y otras, ya que el proxy no puede bloquear en https, puesto que aparece encriptado y no lo puede diferenciar.

Se realizaron los siguientes pasos:

- Acceder al "Cortafuegos"
- Crear reglas de filtrado que "Bloquean protocolos HTTPS".

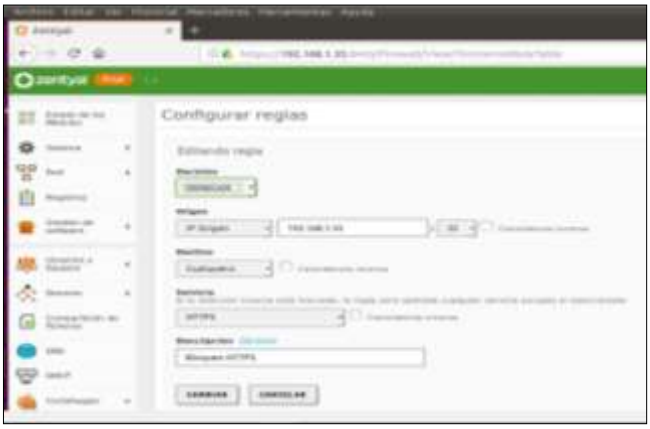

Fig.2 Configuracion de reglas de filtrado.

A partir del uso del Cortafuegos, se pudo bloquear sitios Web como: youtube.com, twitter.com, Instagram.com, y Facebook.com.La siguiente imagen muestra el bloqueo de dos de ellos: youtube.com y Facebook.com:

Fig.3 Configuracion de reglas de filtrado.

Fig.4 Configuracion de reglas de filtrado.

Finalmente, a través del Cortafuegos también se puede permitir el acceso a páginas Web.Para este caso se habilitó el acceso a la página Web de la UNAD, donde se creó una regla nueva para permitir que los usuarios puedan acceder a un sitio en específico y que manejen protocolo seguro HTTPS. Se debe entones entrar a la terminal del sistema operativo Zentyal y realicé un ping a www.unad.edu.co para que retorne la IP y poderla usar, de tal manera que los clientes puedan acceder a la página de UNAD.

Fig.5 Configuracion de reglas de filtrado.

De esta manera, se evidencia que también se puede permitir el acceso a sitios Web a través de dos reglas creadas, por un lado, la de la parte superior es para que los usuarios puedan acceder a https://unad.edu.co. Por otro lado, la regla que se encuentra en la parte inferior corresponde a la antes creada que bloqueará todo los sitios HTTPS.

Fig.6 Configuracion de reglas de filtrado.

C. Implementación de un File Server y Print Server.

Iniciamos instalando dentro de nuestro Virtualbox el servidor Zentyal 5.0.

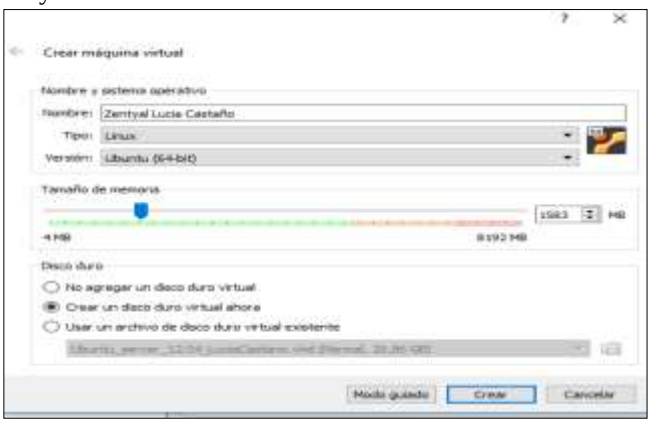

Fig.7 Instalación Zentyal server

El paso siguiente es crear el disco virtual.

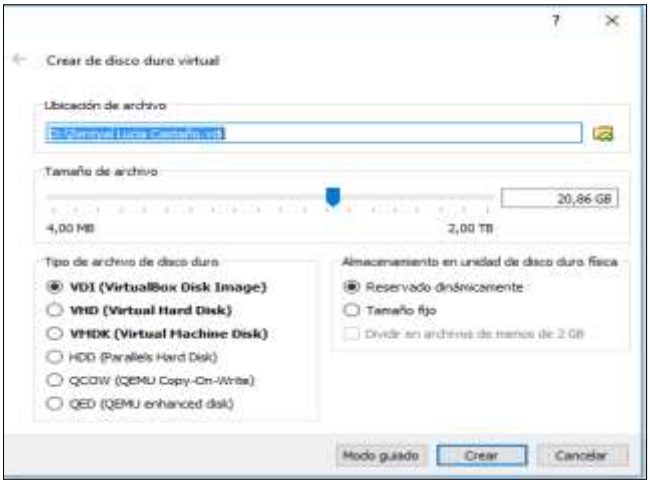

Fig.8 Instalación Zentyal server.

Elegimos la imagen ISO que se va a instalar.

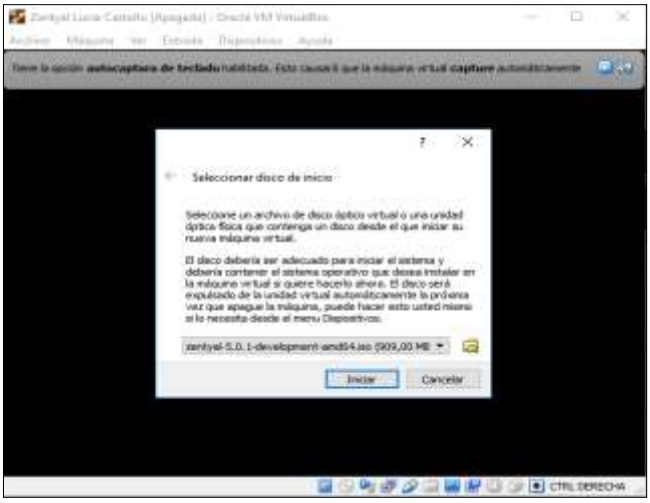

Fig.9 Instalación Zentyal server

Lo siguiente es elegir el idioma, en este caso Español.

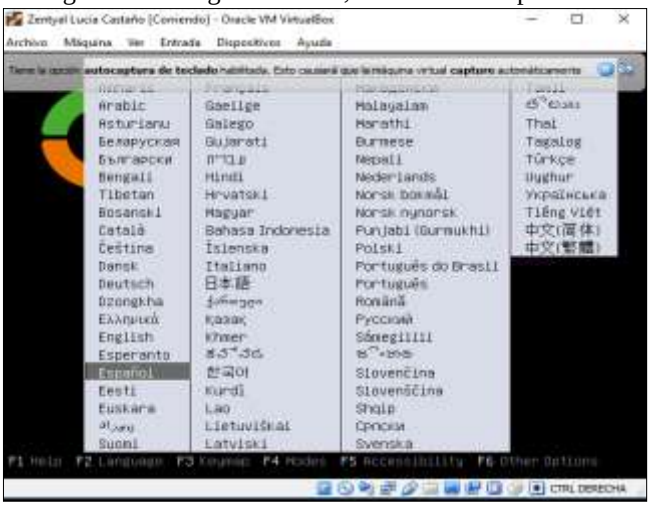

Fig.10 Instalación Zentyal server

Seguimos el asistente de instalación, para este caso se usa todo el disco duro.

Fig.11 Instalación Zentyal server

Seleccionamos el país, en este caso Colombia.

Fig.12 Instalación Zentyal server

Elegimos el teclado de instalación.

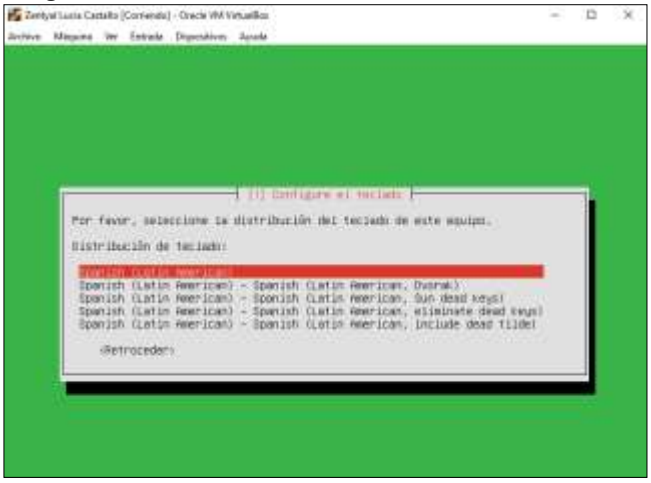

Fig.13 Instalación Zentyal server

Se comienza a realizar la carga de los componentes necesarios para comenzar el proceso de instalación.

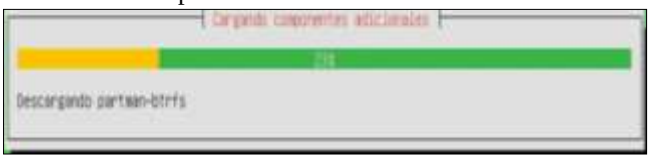

Fig.14 Instalación Zentyal server

Se realiza la configuración del hostname con que quedara configurado el servidor.

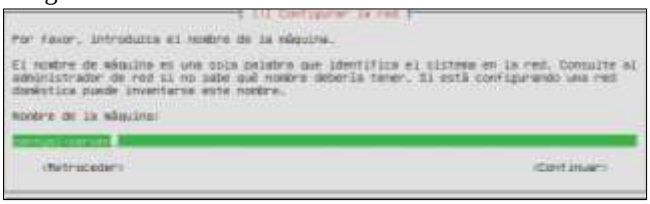

Fig.15 Instalación Zentyal server,
configuración de la máquina.

Se realiza el proceso de la creación de usuarios administradores del sistema.

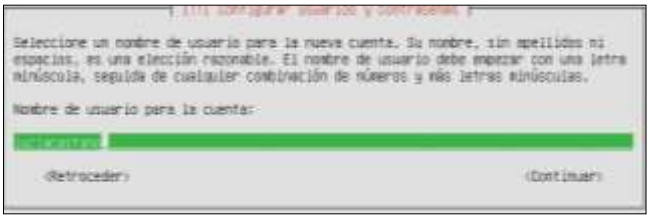

Fig.16 Instalación Zentyal server,
configuración de usuarios

Se asigna una contraseña.

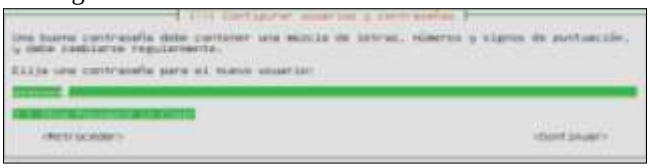

Fig.17 Instalación Zentyal server,
configuración de contraseñas

Comienza el proceso de instalación del sistema, luego se realizará la configuración de los repositorios del servidor Zentyal.

Fig.18 Instalación Zentyal server

Fig.19 Instalación Zentyal server

Una vez instalado Zentyal, nos logueamos a la aplicación y nos aparece la configuración inicial.

Fig.20 Instalación Zentyal server

Instalamos los servicios adicionales o módulos

Fig.21 Instalación Zentyal server

Instalando paquetes seleccionados

Fig.22 Instalación Zentyal server

Se comienza el proceso de configuración de las diferentes interfaces de red, donde indicaremos en primer lugar si la interface es interna o externa, en segundo lugar el método de direccionamiento si es asignado de manera automática o estático que para este caso se seleccionó un direccionamiento dinámico.

Fig.23 Instalación Zentyal server

Fig.24 Instalación Zentyal server

Seleccionamos el tipo de servidor y el nombre que tendrá el dominio y luego de pulsar finalizar comienza a guardar toda la configuración.

Fig.25 Instalación Zentyal server

Un mensaje nos indica que el proceso de configuración se completó de manera exitosa.

Fig.26 Instalación Zentyal server

En la opción del estado de los módulos activamos el módulo recién instalados.

Fig.27 Instalación Zentyal server

Se evidencia cómo se comienza a guardar la configuración seleccionada.

Fig.28 Instalación Zentyal server

Crearemos el recurso compartido desde la opción "Compartición de ficheros", donde indicaremos el nombre del recurso, que será la ruta dentro del sistema y un comentario que es un mensaje descriptivo.

Fig.29 Instalación Zentyal server

Agregamos los usuarios administradores del dominio y los usuarios que iniciaran sesión dentro del dominio.

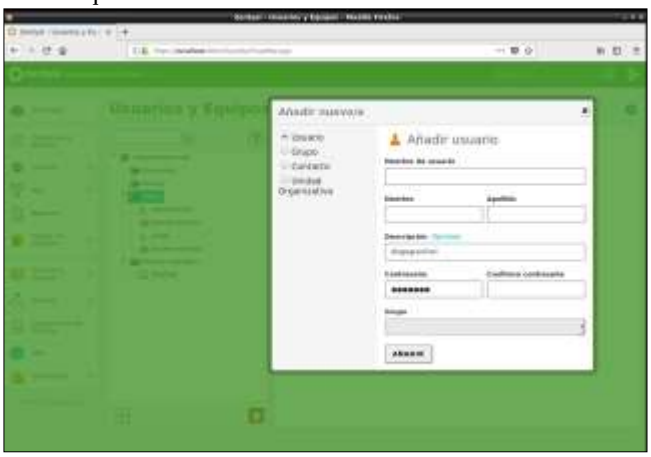

Fig.30 Instalación Zentyal server

Aquí evidenciamos los usuarios creados dentro del dominio.

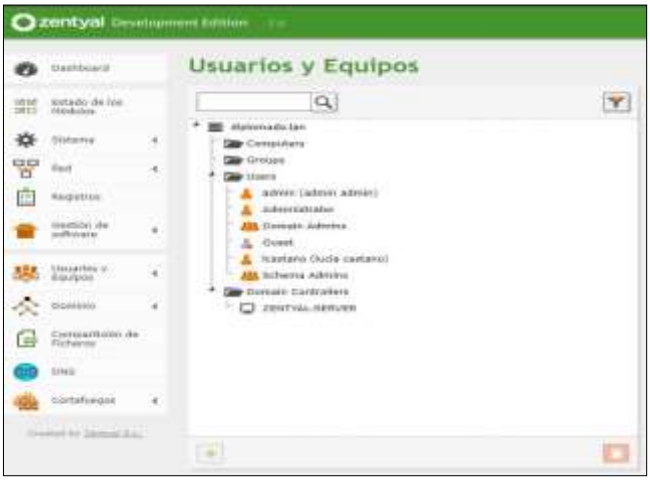

Fig.31 Instalación Zentyal server

Para permitir el inicio de usuario LADP es necesario habilitar la opción de PAM dentro de la configuración del dominio.

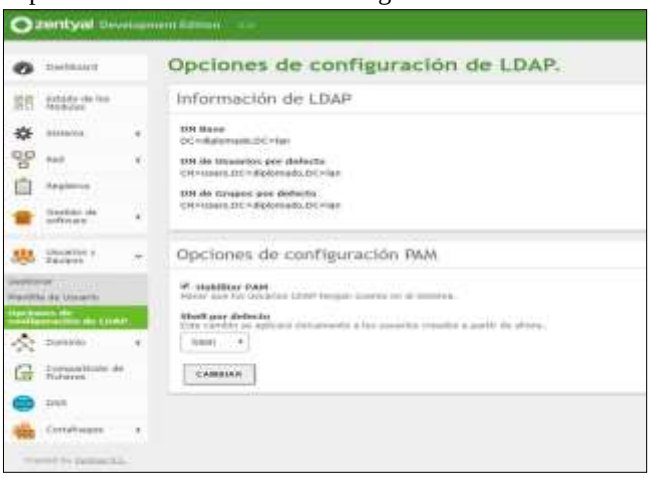

Fig.32 Instalación Zentyal server

Una vez configurado el dominio el necesario configurar el servidor Ubuntu para que acceda al dominio para lo cual se utiliza la aplicación PBIS, lo cual nos permitirá unir la maquina Linux al controlador de dominio.

Realizamos el proceso de descarga del instalador.

Fig.33 Instalación Zentyal server

Asignamos permisos de ejecución al instalador el cual es un script en bash.

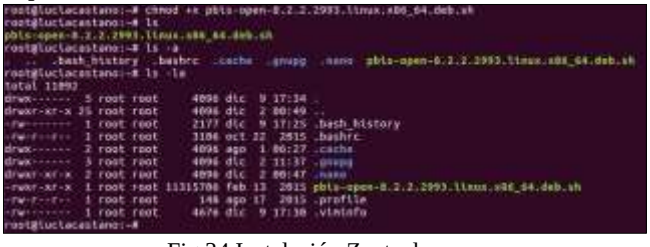

Fig.34 Instalación Zentyal server

Ejecutamos el instalador de la siguiente manera.

Fig.35 Instalación Zentyal server

Debemos agregar la dirección del servidor Zentyal dentro de los servidores DNS del sistema operativo Ubuntu quedando el archivo de la siguiente manera.

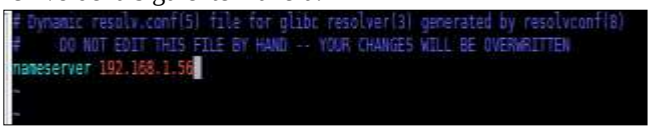

Fig.36 Instalación Zentyal server

Procedemos a agregar la máquina Ubuntu dentro de dominio ejecutando el siguiente comando.

Fig.37 Instalación Zentyal server

Se evidencia que quedó unido correctamente desde Zentyal donde ya vemos el equipo registrado.

Fig.38 Instalación Zentyal server

Es necesario dentro del sistema operativo Ubuntu realizar unas modificaciones es unos archivos de configuración.

Modificar el archivo de configuración lightdm.conf quedando se la siguiente manera.

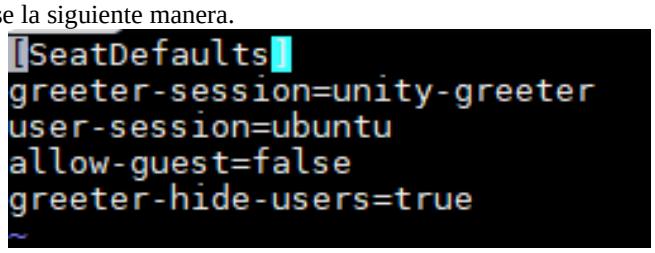

Fig.39 Instalación Zentyal server

Se debe modificar también el archivo de configuración nsswitch.conf quedando de la siguiente manera.

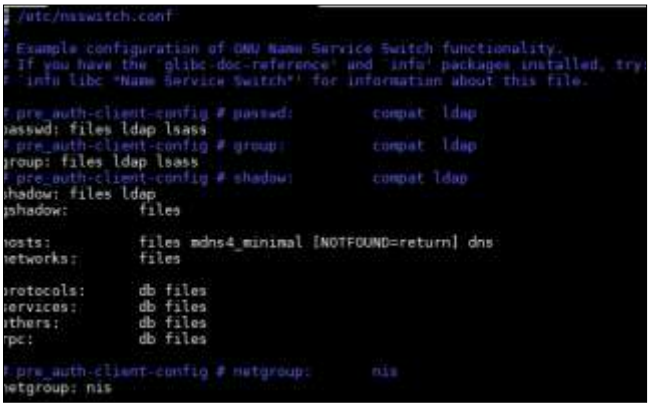

Fig.40 Instalación Zentyal server

Se modifica el archivo de pam common-session como se evidencia a continuación.

Fig.41 Instalación Zentyal server

Utilizamos la herramienta pamtester para validar que el proceso de configuración fue el correcto y se puede iniciar sesión en el dominio.

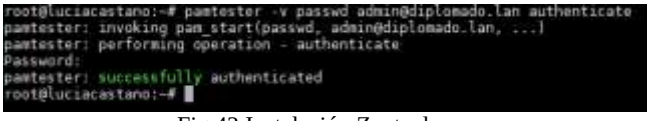

Fig.42 Instalación Zentyal server

Se evidencia el inicio de sesión correcto desde la terminal de Ubuntu desktop como se evidencia a continuación.

Fig.43 Instalación Zentyal server

Fig.44 Instalación Zentyal server

Se evidencia cómo se accede al recurso compartido desde Ubuntu.

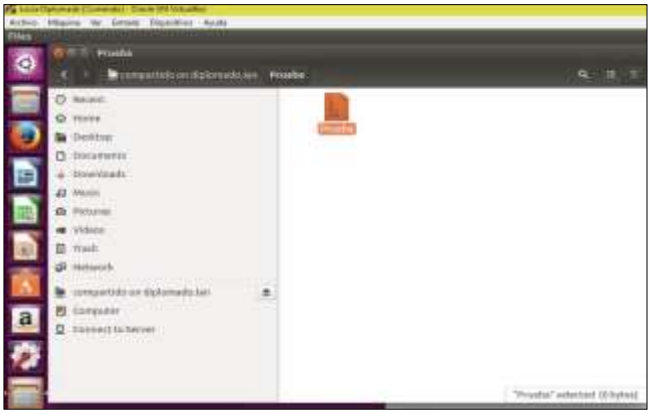

Fig.45 Instalación Zentyal server

D. Configuración del servicio de DHCP

Debemos verificar que el modulo este habilitado.

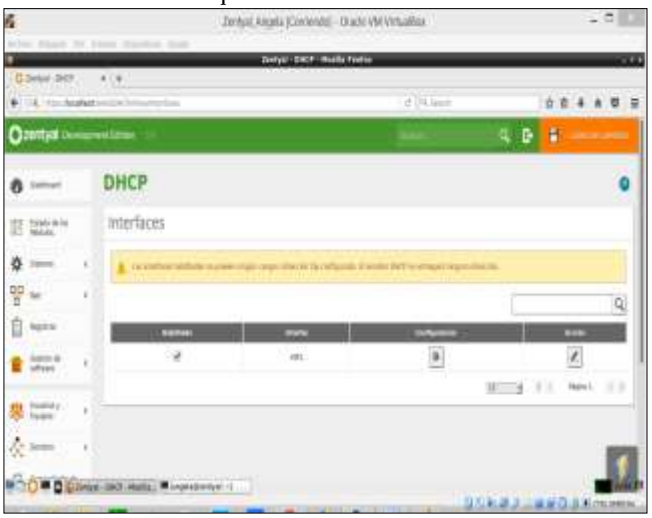

Fig.46 verficacion modulo DHCP

Vamos a la configuración verificamos la ip y el rango disponible la cual vamos a tener disponible desde la dirección ip 1 hasta la 254, es decir vamos a tener disponibles 255 direcciones ip.

Fig.47 configuracion rangos direccion ip

Vamos a añadir el primer rango de dirección ip, y le llamo red local le pongo que empiece de la 150 y que llegue hasta la 170, con el fin de que de 20 direcciones ip.

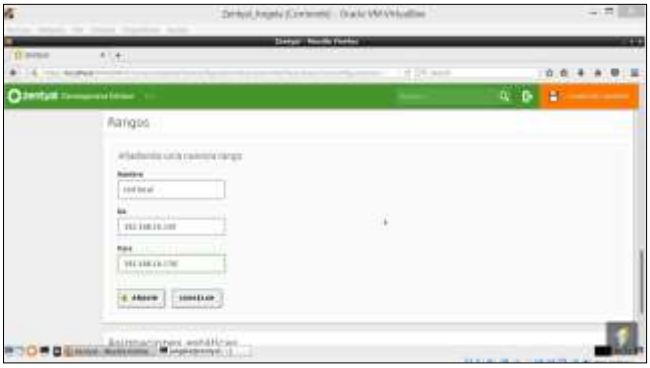

Fig.48 configuracion rangos direccion ip

Clic en añadir y en guardar

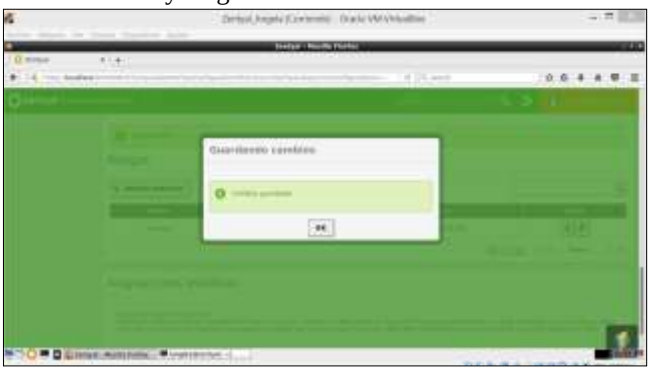

Fig.49 configuracion rangos direccion ip

Realizo una prueba con Ubuntu para verificar si tengo internet

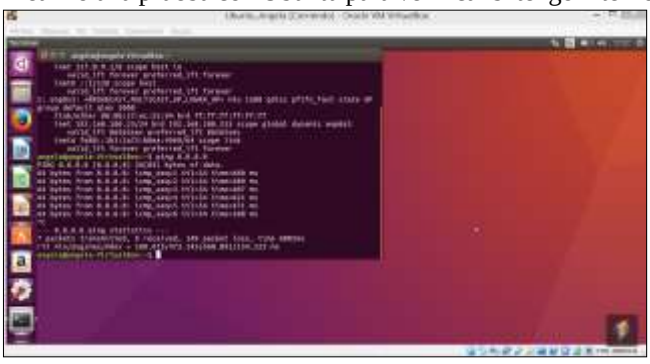

Fig.50 configuracion servicio de red

I. *Configuracion de DNS*

Habilitamos la opción habilitar el cache DNS transparente para que nuestro servidor también resuelva los nombres de dominio y tengamos mayor control sobre nuestra red local

Fig.51 configuracion servicio DNS

II. Configurar Controlador de Dominio

Primero que todo vamos a dominio dejamos la función del servidor como un controlador de dominio y tenemos en cuenta que el reino es lo mismo que el nombre del dominio, además es muy importante habilitar la opción de perfiles móviles para que un usuario se identifique en la red desde cualquier computadora.

Fig.52 configuracion dominio

En usuario y equipo creamos un nuevo grupo llamado unad.

Fig.53 configuracion servicio DNS

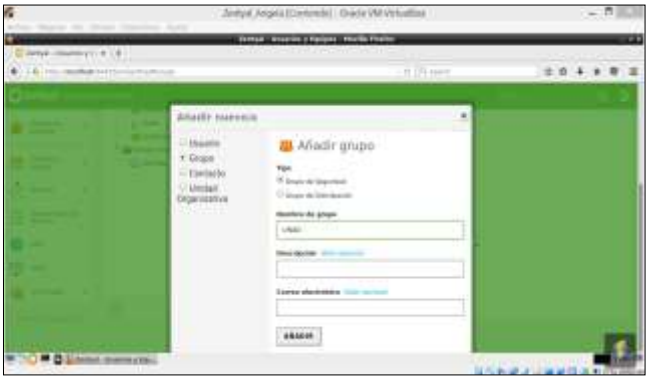

Fig.54 configuracion servicio DNS

Luego creamos un usuario

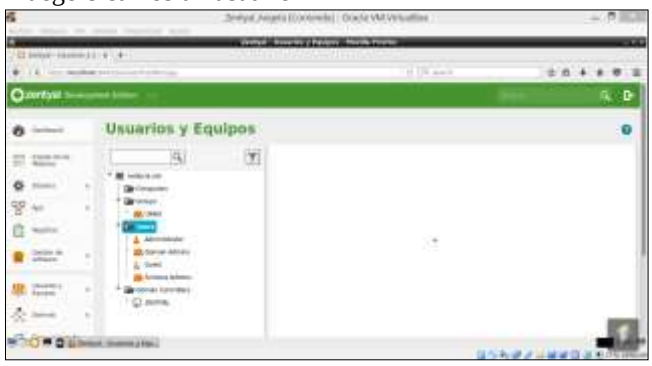

Fig.55 configuracion servicio DNS

Podemos evidenciar que el DHCP está bien configurado, ya que nos registra la conexión de los clientes que se conectan, en este caso el ubuntu desktop.

Fig.56 configuracion servicio DNS

Iniciamos la máquina del cliente Ubuntu, para realizar la correspondiente configuración.

Fig.57 configuracion servicio DNS

Verificamos que nuestro cliente Ubuntu si tiene nternet.

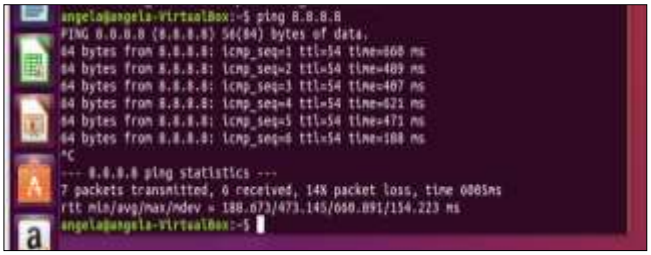

Fig.58 configuracion servicio DNS

Para agregar un usuario Abrimos el active directory donde confirmamos el nombre del dominio, el nombre del usuario que hemos creado anteriormente y guardamos; luego cerramos sección y al volver a abrir nos preguntara con que usuario deseamos ingresar.

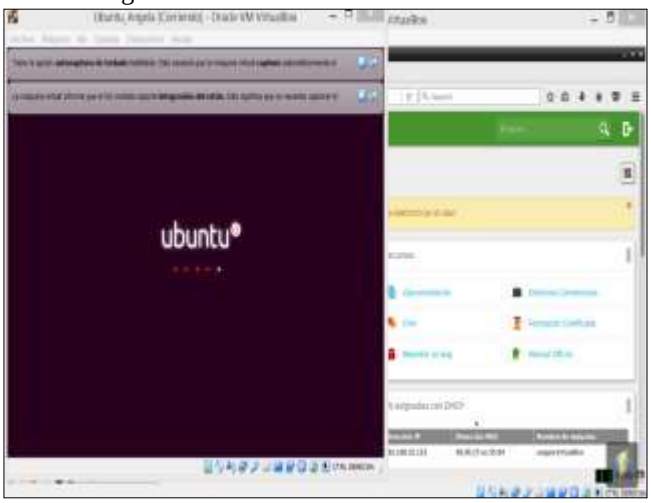

Fig.59 configuracion servicio DNS

E. Implementación y configuración de una VPN.

Para comenzar a desarrollar nuestra temática a profundidad lo que haremos será configurar nuestra VPN desde la Dashboard. Damos clic en aquella opción principal y lo que nos aparecerá será lo siguiente:

Fig.60 configuracion del servicio VPN

La anterior captura mostro el contenido de la subopción Servidores. Estando allí se nos indica que debemos crear un certificado CA para hacer uso de los servidores VPN de manera correcta. Además se nos incida que debemos ir al módulo de autoridad de certificación para crear dicho certificado.

Fig.61 configuracion del servicio VPN

Estando situados ya en la segunda subopción Clientes se nos comparte una opción Añadir Nuevo/a para crear efectivamente un nuevo cliente.

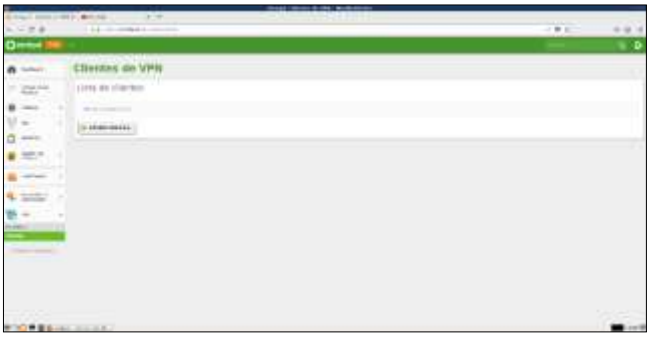

Fig.62 creacion del cliente

Al dar clic en la opción que se nos ofrece, lo que observaremos será un campo para rellenar y una casilla para habilitar. Por último la opción de Añadir o Cancelar.

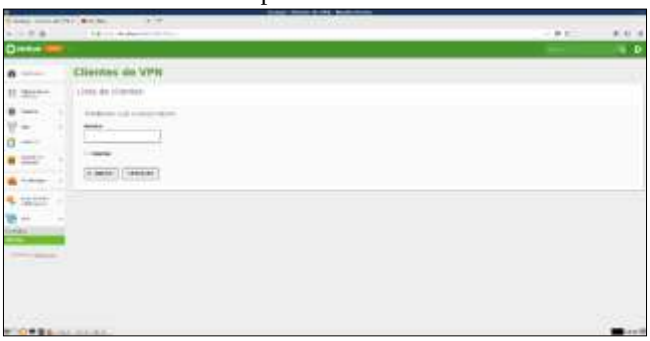

Fig.63 creacion del cliente

Ya para entrar a configurar como tal el servidor VPN lo que haremos será dar clic en la opción módulo de autoridad de certificación. Allí crearemos nuestro certificado de la autoridad de certificación.

Fig.64 creacion del certificado

Nos aparece luego la Lista de Certificados actual que se ha expedido correctamente el certificado, su estado actual es Válido y su fecha de expiración será el 11 de Diciembre de 2027 con su respectiva hora. Además podemos observar tres acciones que se nos ofrecen como son: Revocar, Descargar claves y certificados y Renovar.

Fig.65 creacion del certificado

Posteriormente vamos a la opción principal VPN y allí ingresaremos a la subopción Servidores. Daremos luego clic en la opción *Añadir Nuevo/a* a la Lista de servidores. Al hacerlo también deshabilitaremos la casilla Habilitado y procederemos a poner un nombre al servidor (*Zentyal-Christian*). Daremos luego clic en la opción *Añadir*.

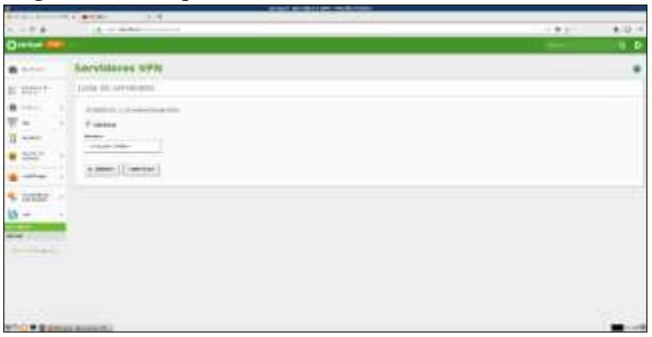

Fig.66 añadir nuevo servidor

Ahora nos dirigimos nuevamente a crear un certificado de autoridad pues el primero que habiamos creado era efectivamente para el Zentyal, lo qe haremos entonces sera crear un nuevo certificado para el servidor que hace un momento creamos, le pondremos como nombre (*certificado-chrisalmanza*) y que este expire en (*mil dias*). Daremos luego clic en la opción *EXPEDIR* y luego guardaremos cambios.

Fig.67 creacion del certificado

Lo que haremos ahora será dirigirnos respectivamente a la opción VPN en la subopción Servidores y allí configuraremos nuestro servidor.

Fig.68 configuracion del servidor

Allí podremos observar la dirección VPN, nuestro certificado de servidor entre otras opciones, es de aclarar que debemos activar la casilla Interfaz TUN, esta sería la única opción que se consideraría necesaria modificar. Al finalizar esto daremos clic en la opción CAMBIAR.

Fig.69 configuracion del servidor

Nos enfocaremos ahora en la conexión que se dará entre el **servidor Zentyal** y la distribución **Ubuntu Cliente**. Nos dirigimos a la opción principal **Red** y allí encontraremos la subopción **Servicios**.

Fig.70 configuracion de servicios

Posteriormente crearemos un nuevo servicio para nuestra conexión **VPN** que estamos llevando a cabo. Para ello daremos clic en la opción Añadir Nuevo/a y una vez lo hacemos pondremos un nombre al servicio y una respectiva descripción. Por último daremos clic en la opción *Añadir*.

Fig.71 creacion de un nuevo servicio

Procedemos entonces a configurar el servicio añadido, iniciando con el protocolo el cual modificaremos por el **UDP** tal cual como nos quedó configurado en el servidor **VPN**. El **puerto de origen** lo dejamos de manera predeterminada (***Cualquiera***) pero en el puerto de destino si modificamos su opción añadiendo el puerto 1194 el cual ya se encontraba previamente definido.

Lo que haremos posteriormente será habilitar el servidor dando clic en la casilla con el nombre de Habilitado.

Fig.72 configuracion del servicio

haremos como un siguiente será el dirigirnos a la configuración del Cortafuegos que nos ofrece el panel de administración de

Zentyal y allí ingresar a su primera subopción Filtrado de paquetes.

Fig.73 configuracion del cortafuegos

Nos involucraremos con la primera opción (*Reglas de filtrado desde las redes internas a Zentyal*) estando allí daremos clic en la opción CONFIGURAR REGLAS. Posteriormente lo que haremos será el dar clic en la opción Añadir Nuevo/a para añadir nuestra nueva regla.

Fig.74 configuracion reglas de filtrado

Configuramos nuesta regla respectivamente colocando en el servicio el que creamos con previa anterioridad (*red-vpn*) y agregamos una descripción (*permisos para puertos OpenVPN*). Luego daremos clic en la opción AÑADIR.

Fig.75 Fig.74 configuracion reglas de filtrado

Volvemos a nuestro servidor VPN ingresando a la subopción Servidores y allí entraremos a la opción Redes anunciadas. Una vez estemos allí daremos clic en la opción AÑADIR NUEVO/A de manera respectiva.

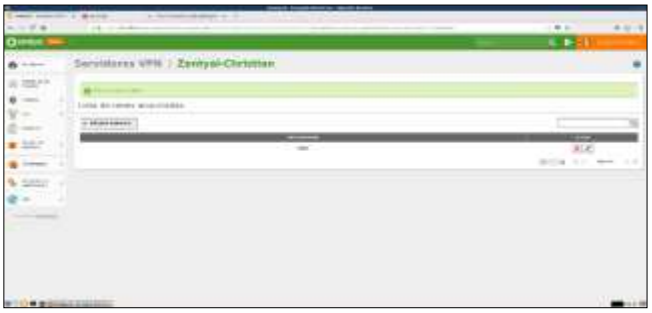

Fig.76 configuracion servidores VPN

Luego ingresaremos a la opción Descargar paquete de configuración de cliente y en esta configuraremos el tipo de cliente (Linux), la estrategia de conexión quedará aleatoria y ponemos la dirección del servidor y una adicional en los campos que allí nos aparecen.

Fig.77 configuracion del cliente

Al finalizar el proceso daremos clic en la opción DESCARGAR y es allí donde se decargara el paquete de configuración en nuestro equipo cliente (Ubuntu Desktop).

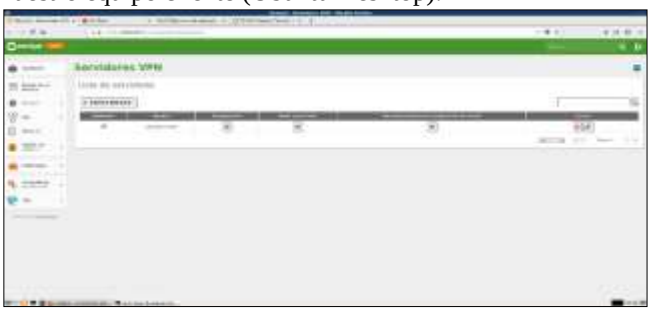

Fig.78 configuracion del cliente

Para verificar que efectivamente la herramienta OpenVPN se está ejecutando correctamente, lo que haremos será irnos a la interfáz principal del panel de administración de Zentyal y verificarlos allí en el espacio de Demonios OpenVPN.

Fig.79 verificacion del servicio

Ahora lo que se hará es ir al S.O. cliente (Ubuntu Desktop) y allí descargar **y** abrir los certificados de Zentyal respectivamente.

Fig.80 configuracion del cliente

Luego se hará el traspaso de los certificados proporcionados por Zentyal a una carpeta que he creado en el escritorio con el nombre de (Certificados Zentyal).

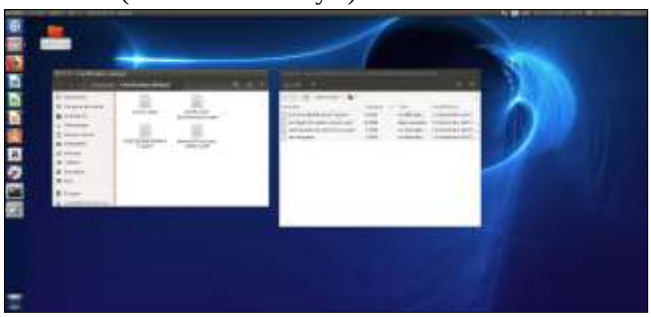

Fig.81 configuracion del cliente

Lo siguiente es instalar la herramienta OpenVPN con ayuda del sistema de configuración Webmin en su versión 1.860. Antes que nada nos vamos a abrir la terminal y digitaremos el siguiente comando "sudo apt-get install openvpn" para ejecutar la instalación de la herramienta.

Fig.82 instalacion OpenVPN

Luego nos vamos a Webmin a la opción Configuración de Webmin y allí ingresaremos a la opción Modulos de Webmin. Una vez allí le damos a la opción Módulo externo desde.

Fig.83 configuracion del Webmin

Se nos cargan luego varias herramientas para lo cual procedemos a buscar la que nos interesa (OpenVPN) al encontrarla detallamos que es la versión 3.1. Luego la cargamos respectivamente y damos clic en la opción Instalar Módulo.

Fig.84 configuracion OpenVPN

Luego nos dirigimos a la opción **VPN List** y creamos nuestro servidor **OpenVPN**, buscaremos para ello el certificado de autorización correspondiente y ahoremos clic en la opción *New VPN server*.

Fig.85 configuracion OpenVPN

Finalmente se logra observar la creación de la herramienta OpenVPN con sus respectivas variables y protocolos de por medio.

Fig.86 configuracion OpenVPN

IV. Conclusiones

- En está actividad se pudo conocer con claridad, cómo controlar la seguridad de una red, desde la instalación del Zentyal y configuración básica de la misma. Logramos completamente la configuración de los paquetes HTTP Proxy, Cortafuegos y DNS para lograr que me generara IP´s dinámicamente.
- Al realizar dicha implementación, reconocemos la importancia del cortafuegos en la medida que a través de este, se puede filtrar el tráfico que intenta salir o entrar de una red donde analiza cada paquete y decide, con base en reglas establecidas, si lo acepta o si lo rechaza.
- La creación de las reglas para bloquear los diferentes sitios web que usan el protocolo HTTP y el Protocolo seguro HTTPS, permite el bloqueo de los sitios de entretenimiento y redes sociales como: www.revistaarcadia.com,www.eltiempo.com,www.twitter.com,www.youtube.com,www.facebook.com.Para la creación de estas reglas y políticas se debe tener en cuenta el modo en que el Zentyal reconoce las reglas; lo cual implica conocimiento amplio de este sistema operativo;si estas reglas se hubieran creado de manera incorrecta, se tendría accesos a todos los sitios Web de entretenimiento. De igual manera, las reglas permiten habilitar sitios con el protocolo seguro HTTPS, evidenciando como ejemplo el sitio web de nuestra universidad. www.unad.edu.co.

- Es necesario e importante tener un dominio efectivo con estas herramientas que nos ayudan a implementar una solución para el manejo adecuado de una red local.

- El uso de cortafuegos es muy importante para empresas como la Aeronáutica Civil, que manejan redes internas con información sensible.

- Conocer las maneras de restringir los sitios Web en una empresa a partir de los protocolos que ellos tienen (HTTP y HTTPS) permitió tomar decisiones efectivas puesto que a través del Módulo HTTP Proxy se pudo restringir sitios Web tales como eltiempo.com y revistaarcadia.com cuyos protocolos son HTTP.Por otro lado, a través del Módulo "Cortafuegos" se restringieron los sitios Web con protocolo HTTPS, tales como : youtube.com, twitter.com

- la configuración de DHCP Server, DNS Server y Controlador de Dominio, ya que es muy importante porque podemos acceder a la información desde cualquier pc de la red.

- Además se pudo identiicar que el servidor DHCP evalúa las directivas de manera secuencial de acuerdo con un orden de procesamiento asignado; es decir el administrador de DHCP es quien asigna el orden de procesamiento a las directivas, por tal motivo si existen directivas de servidor y de ámbito, el servidor aplica ambos conjuntos de directivas y evalúa las directivas de ámbito antes que las directivas de servidor. El orden de procesamiento de una directiva el ámbito define el orden de evaluación dentro del ámbito. Si no hay directivas definidas en el nivel de ámbito, se aplican al ámbito las directivas del nivel del servidor.

- Por otra parte hay que tener en cuenta que para realizar estas configuraciones se debe tener un excelente equipo que soporte las maquina virtuales corriendo al mismo tiempo.

- Es de aclarar que la información que se recopilo fue de gran ayuda para el desarrollo oportuno de la actividad planteada. Las fuentes tales como videos en linea, documentos en formato PDF y articulos web, ayudarón a esclarecer los posibles pasos que se debierón aplicar para la correcta funcionalidad de la VPN al crear y evidenciar un tunel de comunicación entre las distribuciones Zentyal Server y Ubuntu Desktop en su versión 16.04.

V. Referencias

Sitio oficial de descarga del Zentyal 5.0.1. 2017. Recuperado de: http://www.zentyal.com/es

Sitio oficial de documentación Zentyal Firewall. 2017. Recuperado de: https://wiki.zentyal.org/wiki/En/5.0/Firewall

Sitio oficial de documentación Zentyal Cortafuego. 2017. Recuperado de: https://wiki.zentyal.org/wiki/Es/5.0/Cortafuegos#configuracion-de-un-cortafuegos-con-zentyal

Sitio oficial de documentación Zentyal, Servicio de Proxy HTTP.2017. Recuperado de: https://wiki.zentyal.org/wiki/Es/5.0/Servicio_de_Proxy_HTTP#reglas-de-acceso

Es/3.5/Servicio de Proxy HTTP.2014. Recuperado de: https://wiki.zentyal.org/wiki/Es/3.5/Servicio_de_Proxy_HTTP

Es/3.5/Cortafuegos.2014.Recuperado de: https://wiki.zentyal.org/wiki/Es/3.5/Cortafuegos

Pasamar. Daniel.Zentyal: Configuración de Proxy Transparente.2014.Recuperado de: http://cerowarnings.blogspot.com.co/2012/04/zentyal-configuracion-de-proxy.html

Análisis de aplicación: Cortafuegos de la distribución Zentyal.Centro de Apoyo Tecnológico a Emprendedores.2011.Recuperado de: https://www.bilib.es/fileadmin/user_upload/analisis-bilib-zentyal.pdf

Es/5.0/Instalacion. Recuperado de:https://wiki.zentyal.org/wiki/Es/5.0/Instalacion

Zentyal – Controlador de Dominio Linux y Politicas de Grupo. Recuperado de: https://juliorestrepo.wordpress.com/2015/02/09/zentyal-controlador-de-dominio-linux-y-politicas-de-grupo/

Articulo web titulado "ZENTYAL ANUNCIA EL SERVIDOR ZENTYAL 5.0". Publicado por la red de Partners de Zentyal por medio del sitio web "zentyal.com", el 26 de Enero de 2017. Extraído el 12 de Diciembre de 2017, http://www.zentyal.com/es/press/zentyal-announces-zentyal-server-5-0/

Mora, A. (2017). *Intalación Zentyal 5.0.* [*Video*]. Disponible en: https://youtu.be/5N9upYznnCo

Rodríguez, R. (2015). *Configuración y conexión a un servidor VPN con Zentyal usando OpenVPN*. [*Video*]. Disponible en: https://youtu.be/3rNfipxE-9o

Turner-Benites, C. A. (2017). *Configuración de VPN en Zentyal*. [*Video*]. Disponible en: https://youtu.be/qp9UhuRSBcc

Morán, J. (2015). Zentyal VPN. [Video]. Disponible: https://youtu.be/XeIxNWQ6zFA

Vasquez, P. (2012). Conexion VPN Zentyal. [Video]. Disponible: https://youtu.be/XzuyTYUOmBU

Luis Fernando Molina. Estudiante de último semestre del programa de Ingeniería de Sistemas en el CEAD Florencia de la Universidad Nacional, Abierta y a Distancia. Actualmente labora en la empresa SOLINFO. Ha trabajado como diseñador gráfico de periódicos en Florencia- Caquetá.

Lucia Castaño Marín (Medellín, 1985) Estudiante de último semestre del programa de Ingeniería de Sistemas en el CEAD Medellín de la Universidad Nacional Abierta y a Distancia. Actualmente labora en Ceipa Business School como Administradora e-learning.

Mis estudios incluyen:

- Técnica en Sistemas, Centro de estudios en sistemas – CES.Medellín 2005
- Tecnóloga en Sistemas, Tecnológico de Antioquia - T de A. Medellín 2008
- Ingeniería en Sistemas, Universidad Nacional Abierta y a Distancia – UNAD. Medellín 2018

Gerardo Ramos Jara. (Florencia, 1994) Integrante del programa de Ingeniería de Sistemas, perteneciente a la Escuela de Ciencias Básicas, Tecnología e Ingeniería (ECBTI) de la Universidad Nacional Abierta y a Distancia - UNAD, aspirante al título de Ingeniero de Sistemas.

Mis estudios incluyen:

1. Técnico en Sistemas de Información, Instituto de Educación para el Desarrollo Humano "COMFACA", Florencia – Caquetá, Colombia, 2011.
2. Tecnólogo en Análisis y Desarrollo de Sistemas de Información, Centro Tecnológico de la Amazonia "SENA", Florencia – Caquetá, Colombia, 2013.
3. Especialización Tecnológica en Gestión y Seguridad de Bases de Datos, Centro Tecnológico de la Amazonia "SENA", Florencia – Caquetá, Colombia, 2015.

Christian Ricardo Almanza Castañeda (***07 de Diciembre de 1994***). Estudiante perteneciente al programa de pregado Ingenieria de Sistemas, actualmente matriculado en el CEAD Acacias de la Universidad Nacional Abierta y a Distancia (***UNAD***).

Se encuentra en el momento dedicado al ámbito académico cursando dos diplomados relacionados con los temas tales como: Desarrollo Web y Móvil. Prestó reciententemente sus servicios como e-monitor académico en la institución de educación superior.

Angela Maria Mejia Gaez (***09 de octubre de 1990).*** Estudiante del programa Ingenieria de Sistemas, perteneciente a la Universidad Nacional Abierta y a Distancia (UNAD) en el CEAD de Santander de Quilichao. Actual mente soy comerciante Independiente.

Mis estudios incluyen:

- Tecnóloga en Sistemas de Informacion, Tecnológica Autonoma del Pacifico – Cali – Valle, Colombia, 2015
- Diplomado en Redes, Tecnológica Autonoma del Pacifico – Cali – Valle, Colombia, 2016