

INSTALACION Y CONFIGURACION DE SERVICIOS DE INFRAESTRUCTURA DE RED MEDIANTE SOFTWARE LIBRE

Carlos Hernán Moreno Pérez
c.h.morenoperez@gmail.com
Carolina Arroyave Cardona
carroyaveca@unadvirtual.edu.co
Jhonatan Grueso Perea
Jhonper86@gmail.com
Antonio John James Lopez
anjoalo1@gmail.com

RESUMEN: *El software libre se posiciona como un elemento clave en los servicios de redes, sin embargo, se cuenta con poca información sobre los servicios que bajo este sistema operativo se pueden instalar. El objetivo de este documento, es la de mostrar la configuración básica y puesta en marcha de servicios de red, mediante el uso de un programa de virtualización en la que se instala el sistema operativo de distribución Linux.*

ABSTRACT: *Free software is positioned as a key element in network services, however, there is little information on the services that can be installed under this operating system. The objective of this document is to show the basic configuration and start-up of network services, through the use of a virtualization program in which the Linux distribution operating system is installed.*

PALABRAS CLAVE: Software libre, servicios de red, Proxy, Cortafuegos, VPN.

1 INTRODUCCIÓN

Con el aumento de servicios de red que han proliferado en los últimos años, es de entender que, las pequeñas y medianas empresas necesiten posicionarse con los servicios necesarios en las intranets. No es de extrañar que partes de las empresas tengan pensado en agregar varios de estos servicios, la pregunta que surge con esta iniciativa, ¿qué software existe en el mercado? Y por omisión o falta de información, la mayoría de personas optan por la instalación de software privativo, pero sin entender que también está la opción de software libre. Una de las creencias que sustentan el no instalar software libre, es la complicada puesta en marcha, instalación y usos ya preestablecidos en otro tipo de versiones.

En este trabajo se dio una descripción, de los diferentes servicios que se pueden instalar con software libre como pueden ser: DHCP, DNS, Proxy, Firewall, Controlador de dominio y VPN.

En la primera parte del trabajo se destina a mostrar toda la instalación del sistema base, optando por utilizar

una distribución Zentyal, programa que está dirigido a pymes, estando de por medio su fácil instalación y configuración de los servicios.

En la segunda parte del trabajo se han mostrado las diferentes configuraciones, DHCP server, DNS server, controlador de dominio Proxy no transparente, Firewall, servidor de archivos e impresoras y por último VPN.

2 METODOLOGIA

2.1 MATERIALES

Computador en condiciones estables con suficiente memoria RAM, Disco duro, Tarjeta de red.

Como elemento de pruebas se ha usado software de virtualización VirtualBox del fabricante Oracle, que permite la instalación y emulación de las partes iniciales para el hospedaje de un sistema operativo.

En el software libre, se ha utilizado una distribución Linux Zentyal 6.1, que del mismo modo está basada en Ubuntu.

En el caso de los host o sistemas de prueba se ha usado distribución Debian de Linux.

2.2 CONFIGURACIÓN Y PRUEBAS

Una vez instalado el software base: Zentyal 6.1, se agregaron los respectivos servicios de: DHCP, DNS, Proxy, Firewall, Controlador de dominio y VPN. Al término de la configuración de los servicios, las pruebas se realizaron con los respectivos host, bajo el sistema Debian 10.

2.3 RESULTADOS

En las diferentes configuraciones se comprobaron los servicios de DHCP, DNS, Proxy, Firewall, Controlador de dominio y VPN.

3 TEMATICA 1: DHCP SERVER, DNS SERVER Y CONTROLADOR DE DOMINIO.

Producto esperado: Implementación y configuración detallada del acceso de una estación de trabajo GNU/Linux Debian 10 a través de un usuario y contraseña, así como también el registro de dicha estación en los servicios de Infraestructura IT de Zentyal

Configuración de las interfaces red
Red 1 eth0 en modo DHCP



Figura 3.1. Red eth0 en modo DHCP

Red 2 eth1 en modo estático IP 192.168.70.10
mascara de red 255.255.255.0



Figura 3.2. Red eth1 en modo estático

Activamos los módulos de DHCP para generar la IP sobre otra máquina virtual por red interna

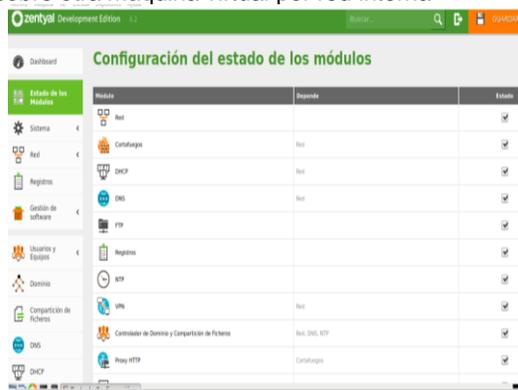


Figura 3.3. Activación del módulo DHCP

Luego mostramos la IP que sería 192.168.42.15 que ha sido definida por el servidor.

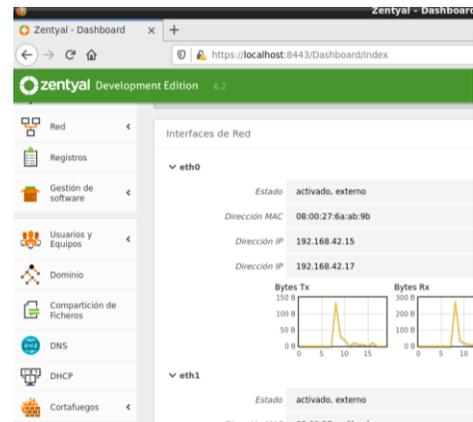


Figura 3.4. Activación para comunicación servidor

Miramos que en dashboard no hay ninguna IP asignada en el DHCP al cliente Debian 10.

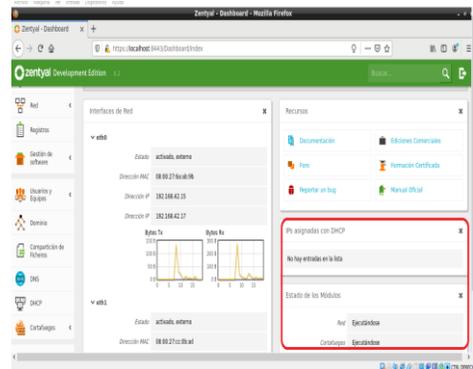


Figura 3.5. Validación de ip DHCP

Procedemos a la configuración de desde el módulo DHCP donde encontraremos la interfaz eth0 para asignar la IP a nuestro cliente (debian 10).

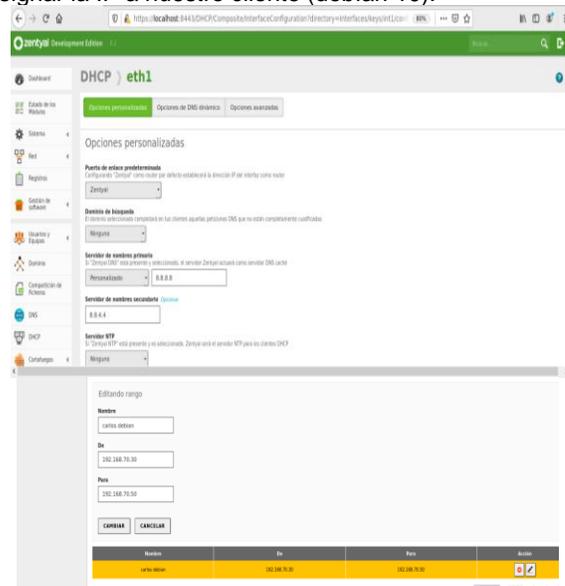


Figura 3.6. Configuramos el rango que va ir desde la IP 192.168.70.30 a la IP 192.168.70.50

Ahora abrimos debian 10 y verificamos la IP que fue asignada por DHCP

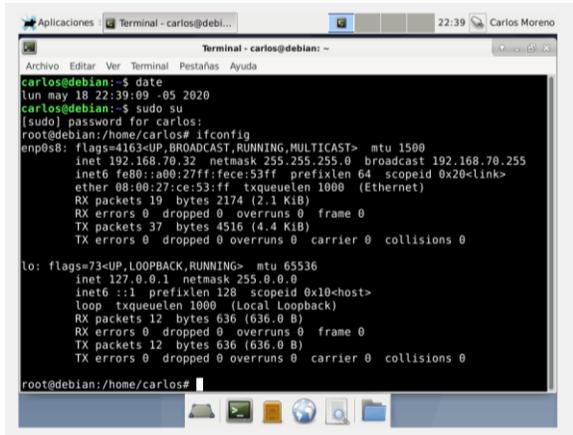


Figura 3.7. Verificación de IP en la terminal de debían 10

Ahora verificamos en el dashboard que la IP 192.168.70.32 fue asignada a nuestro cliente Debían 10

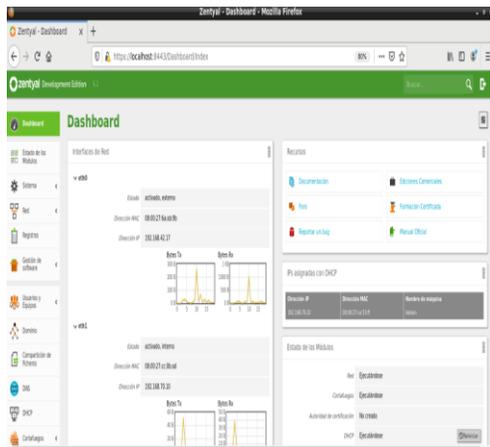


Figura 3.8. Verificación en Dashboard de la IP asignada

Activamos el módulo DNS como transparente y añadir un nuevo dominio.

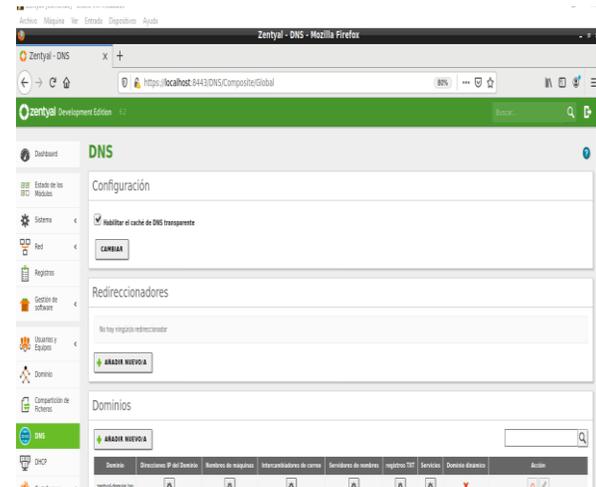


Figura 3.9. Configuración y activación del dominio

Verificamos que debían 10 ya tiene activo el DNS

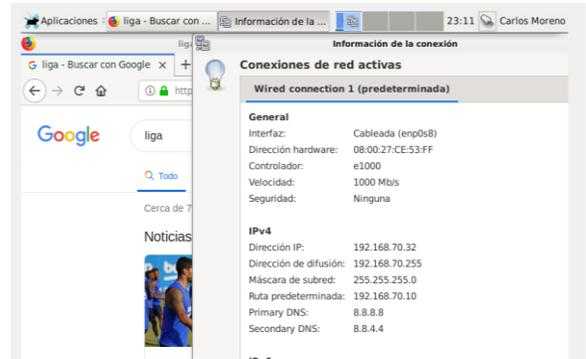


Figura 3.10. Verificación DNS

Configuramos nuestro servicio de controlador de dominio LDAP el cual ya se había especificado la instalación del módulo junto con el DHCP y DNS anteriormente.



Figura 3.11. Configuramos nuestro servicio de dominio

Activamos el dominio en el estado de los módulos.



Figura 3.12. Activación modulo dominio

Verificamos la configuración del módulo LDAP de dominio en Zentyal.

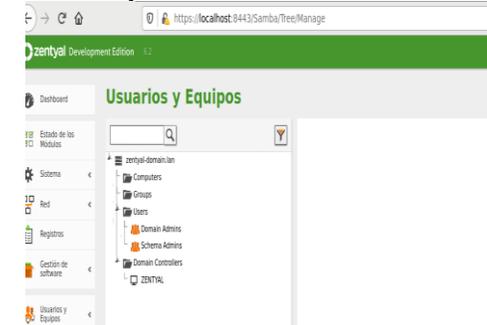


Figura 3.13. Verificación de control de dominio

4 TEMATICA 2: PROXY NO TRANSPARENTE

Para esta sección se implementa y configura de manera detallada el control del acceso de una estación GNU/Linux Ubuntu Desktop a los servicios de conectividad a Internet desde Zentyal a través de un proxy que filtra la salida por medio del puerto 3128.

Se elige el tipo de configuración necesario para la actividad.



Figura 4.1. Configuración de Interfaces



Figura 4.2. Configuración de Redes

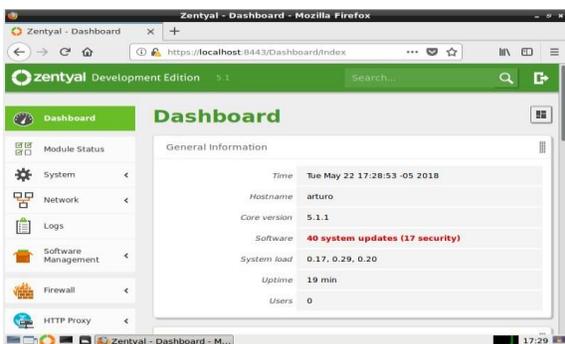


Figura 4.3. Ingreso a Dashboard

En este momento ya podemos iniciar sesión con el usuario creado en Zentyal.



Figura 4.4. Configuración de Interfaces

Dentro de la configuración de Zentyal hay dos configuraciones de red. Una de las redes es la red WAN la cual es de internet y la otra interfaz es de la red LAN, donde está conectada la máquina de Ubuntu. La IP de la red LAN es la siguiente 192.168.0.1. Y la red WAN está configurada por DHCP.

A continuación, se muestra la configuración de la red LAN.

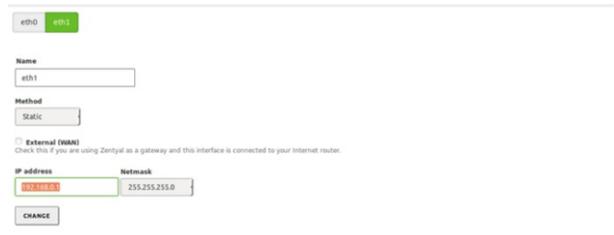


Figura 4.5. Configuración de Red WAN

Para realizar los requerimientos de temática entramos a HTTP Proxy opción General Settings.

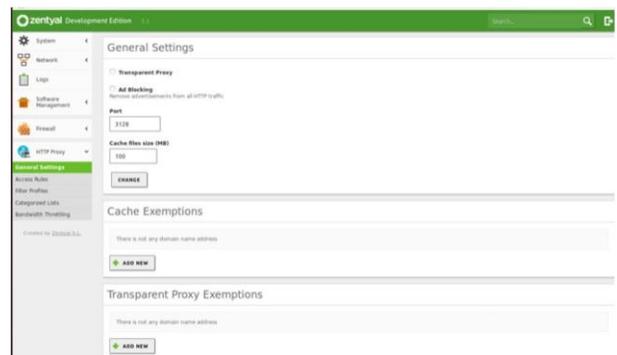


Figura 4.6. Configuración de HTTP Proxy

Se debe habilitar el proxy en el Zentyal y se entra al Module Status y se le da clic al checkbox de HTTP Proxy y guardamos los cambios.



Figura 4.7. Habilitar de HTTP Proxy

Nos vamos a Firefox de la máquina de Ubuntu para realizar la configuración del Proxy.

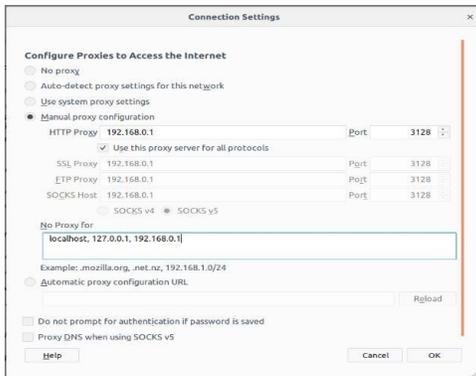


Figura 4.8. Configuración de Proxy en Firefox

Se prueba en el Ubuntu de escritorio que ingrese una página, por ejemplo, Google.

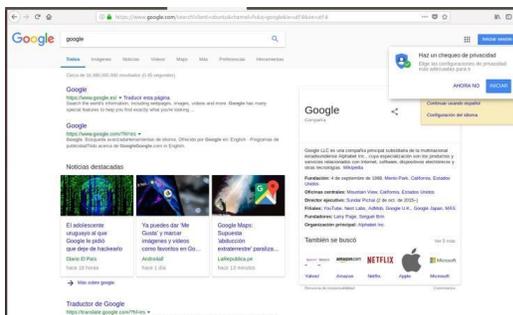


Figura 4.9. Prueba de Proxy por puerto 3128

Si queremos bloquear por ejemplo la página de google.com.

Nos vamos a HTTP Proxy opción FilterProfiles

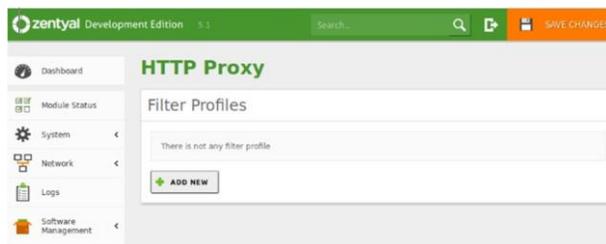


Figura 4.10. Filtros de HTTP Proxy

Ahora estando aquí le damos en Add New y creamos nuestro filter.



Figura 4.11. Adicionar Filtros de HTTP Proxy

Le damos click al botón de configuración y nos aparece esta ventana.

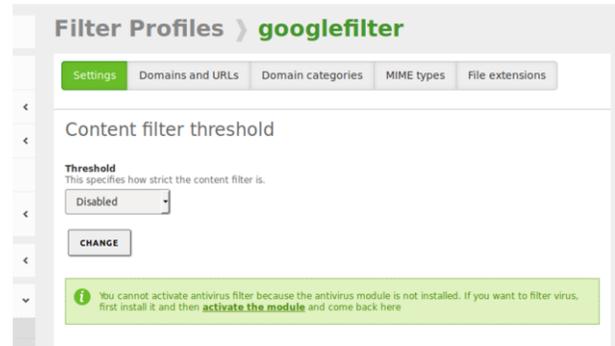


Figura 4.12. Configurar Filtro creado

Le damos clic a "Domains and URLs".

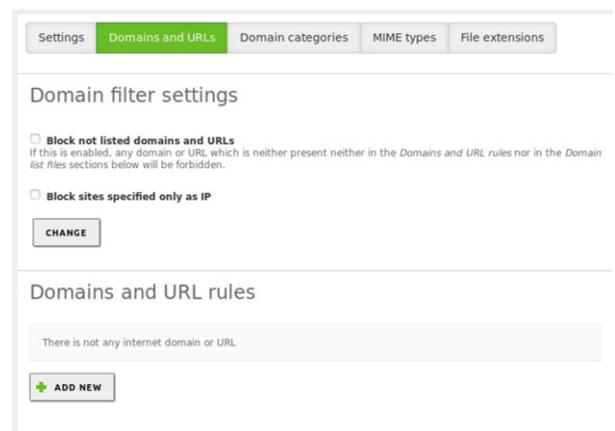


Figura 4.13. Creando Dominios y Reglas

Le damos AddNew.

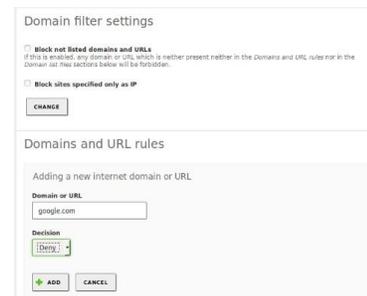


Figura. 4.14. Configurar Filtro creado con Deny

Probamos y efectivamente esta denegado el acceso

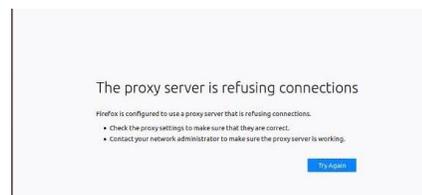


Figura 4.15. Prueba de bloqueo HTTP Proxy

5 TEMÁTICA 3: CORTAFUEGOS

Un cortafuegos, se define como un servicio de red que, permite el bloqueo de diferentes tipos de tráfico de red, posibilitando aumentar la seguridad de este e impedir que personas o servicios pueden ingresar a las redes internas. Este servicio se puede presentar en un solo dispositivo o el uso de varios cortafuegos.

En esta implementación se ha configurado un cortafuegos, software de distribución Linux Zentyal 6.1, en la que se realizó una configuración inicial de una red LAN y una red DMZ. Su cometido final para esta empresa es, la de poder bloquear sitios de entretenimiento como pueden ser; Facebook, Twitter y otras páginas que se requieran.

Para la configuración inicial se debe descargar la versión de Zentyal 6.1 y como la mayoría de sistemas operativos de la distribución Linux, se debe instalar bajo ciertos parámetros, siguiendo pasos básicos como son: asignación de un dispositivo con capacidad de memoria RAM, disco duro, 3 puertos ethernet (uno para la salida a la WAN, otro para la red LAN y el último para la zona DMZ) para la simulación de todas las partes se ha utilizado software de virtualización VirtualBox para contar con las características anteriormente nombradas.

Ya con una configuración previa de estas particularidades, el sistema de instalación sigue una pautas de elección de idioma, tipo de teclado, configuración y detección de los puertos de red, asignación de nombre de la máquina, nombre de usuario para una cuenta y del mismo modo una clave para esta cuenta, sistema horario que se detecta automáticamente en la mayoría de los casos, un sistema de particionado de discos ya sea manual o guiado, instalación de entorno gráfico, instalador de arranque y que este sería el paso final para la instalación base del sistema operativo.



Figura 5.1. Componentes básicos de Hardware

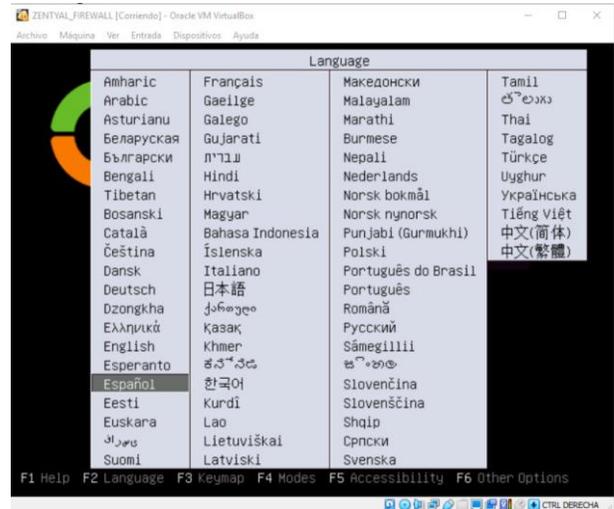


Figura 5.2. Elección de idioma



Figura 5.3. Configuración tarjetas de red

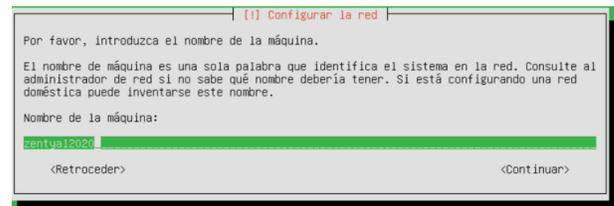


Figura 5.4. Asignación nombre de la máquina

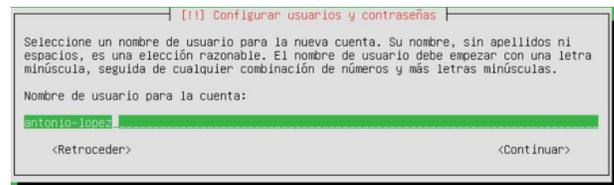


Figura 5.5. Asignación usuario de la cuenta

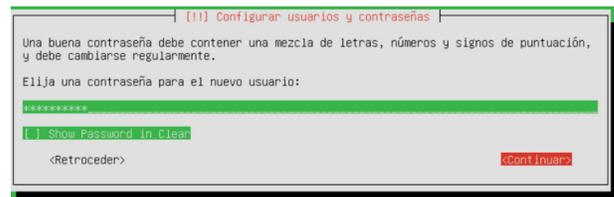


Figura 5.6. Asignación clave usuario

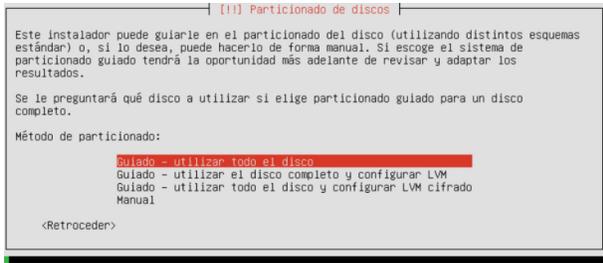


Figura 5.7. Tipo de particionado (discos duros)

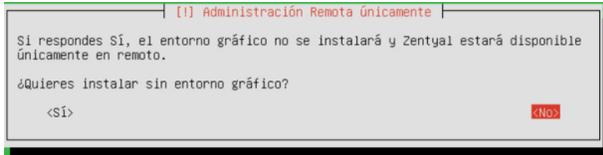


Figura 5.8. Elección con o sin entorno gráfico

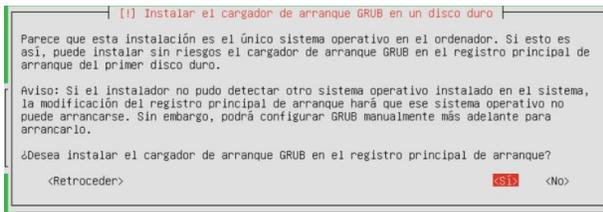


Figura 5.9. Instalación gestor de inicio GRUB

5.1 INSTALACION DE SERVICIOS

Una vez instalado el sistema base, se deben instalar los servicios, en el caso del cortafuegos es indispensable agregar otros módulos como es el de DHCP, para la asignación de direcciones de las demás redes.



Figura 5.1.1. Seleccionar servicios a instalar



Figura 5.1.2. Configuración puerto eth1



Figura 5.1.3. Configuración puerto eth2

5.2 CONFIGURACION FIREWALL

La configuración de este firewall ofrece diferentes alternativas, la que se ha utilizado para el desarrollo de esta actividad es, la de bloquear la salida hacia ciertas páginas. En el módulo reglas de filtrado para redes internas se configuran, ubicando el origen, destino y bloqueando los servicios necesarios.



Figura 5.2.1. Módulos para diferentes reglas



Figura 5.2.2. Asignación y configuración de reglas

6 TEMATICA 4: FILE SERVER Y PRINT SERVER

El servidor de archivos o más conocido como Active Directory, permite a los usuarios compartir carpetas en una red, mediante el uso de un servidor de domino. En este mismo concepto también se ha trabajado con un servidor de impresoras, haciendo uso de este servicio en Zentyal. Cabe aclarar que las versiones a partir de: 5.0 en adelante, no tienen este servicio.

En el caso de la instalación de Zentyal 4.1, no cambia en su metodología de instalación.

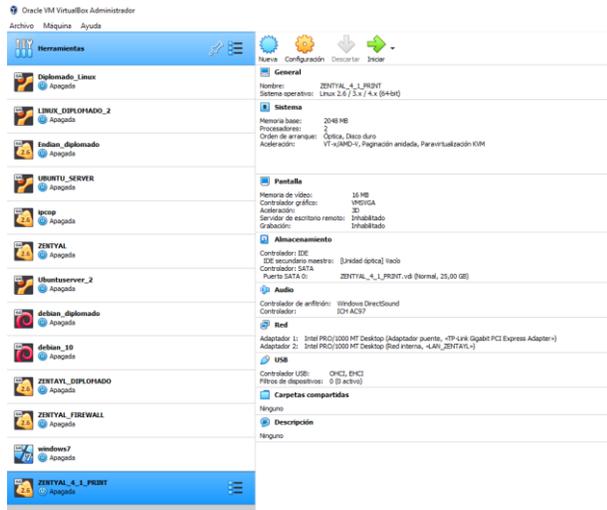


Figura 6.1. Componentes básicos de Hardware

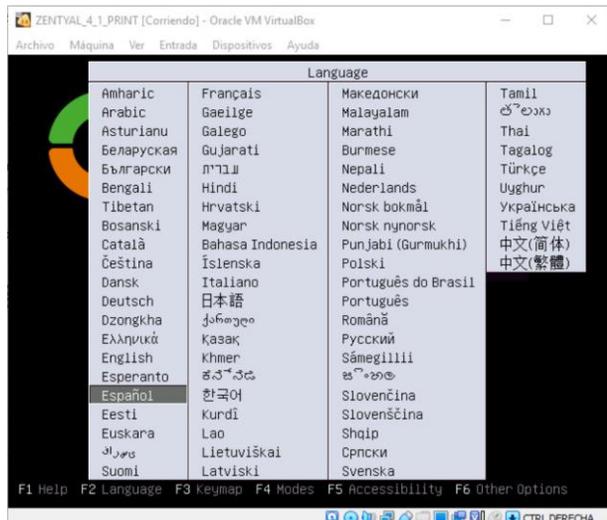


Figura 6.2. Elección de idioma

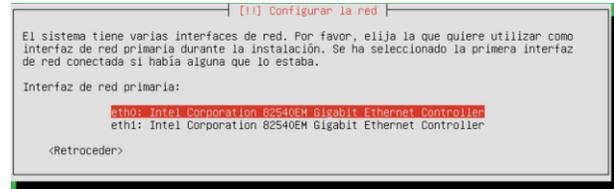


Figura 6.3. Configuración tarjetas de red

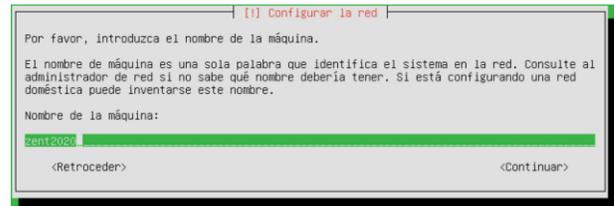


Figura 6.4. Asignación nombre de la máquina

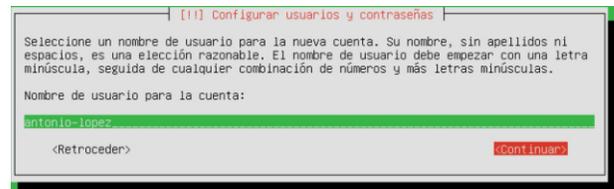


Figura 6.5. Asignación usuario de la cuenta

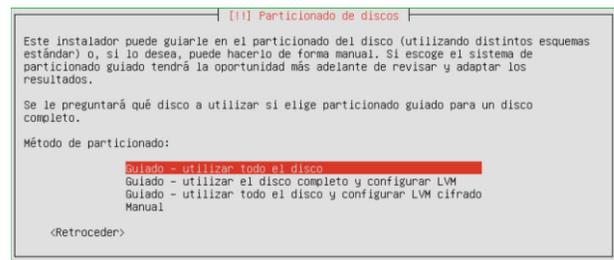


Figura 6.6. Tipo de particionado (discos duros)

6.1 INSTALACION DE SERVICIOS

Después de la instalación base, es necesario agregar los servicios, el controlador de dominio depende de varios servicios adiciones como pueden ser: DHCP, Firewall, DNS server, controlador de dominio de archivos e impresoras.



Figura 6.1.1. Seleccionar servicios a instalar

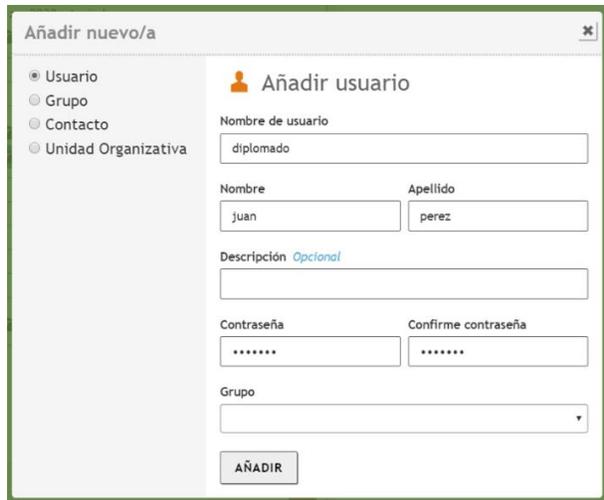


Figura 6.1.2. Añadir usuario

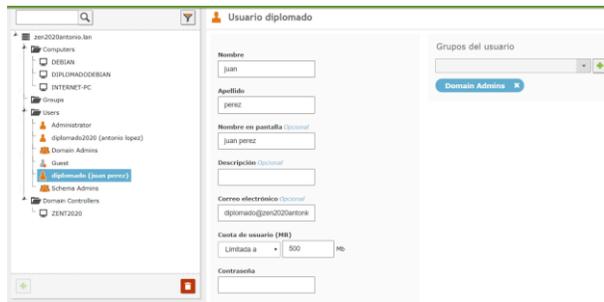


Figura 6.1.3. Añadir usuario a un grupo

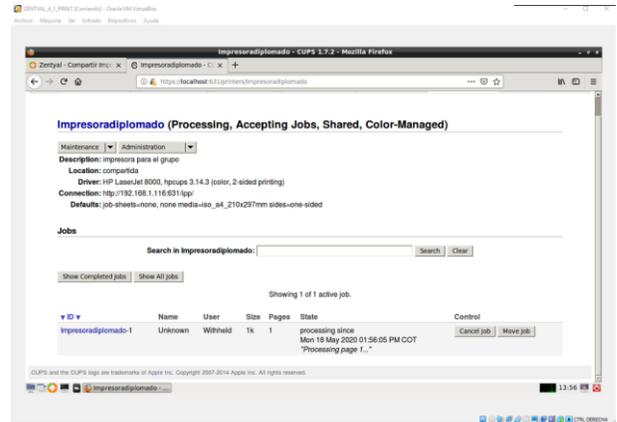


Figura 6.1.5. Instalación impresora



Figura 6.1.6. Acceso de usuario "diplomado"

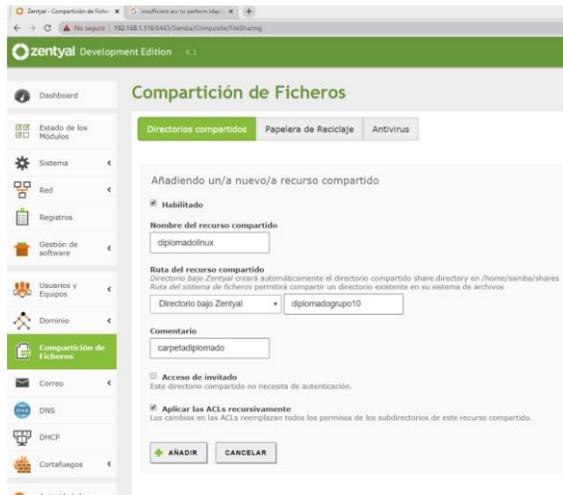


Figura 6.1.4. Añadir carpeta

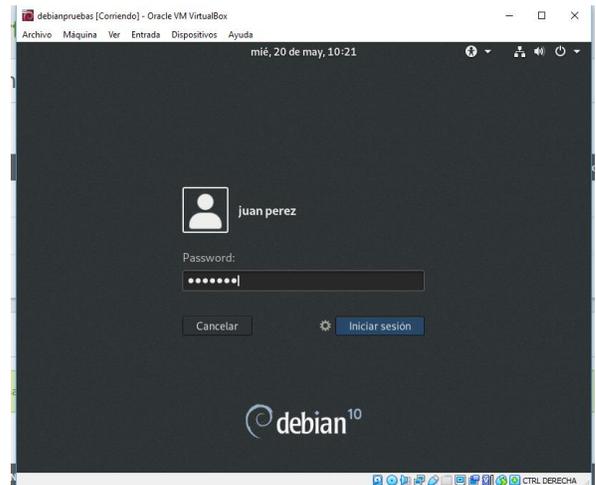


Figura 6.1.7. Cierre de sesión e ingreso al dominio

7 TEMATICA 5: VPN

7.1 PROCESO DE INSTALACION

Como primer paso, se debe descargar la imagen ISO desde el siguiente sitio web <https://zentyal.com/community/>. Dado que Zentyal requiere actualizar a la última versión se hizo la instalación de la versión 6.2. La configuración que deberá tener la máquina virtual box, será:

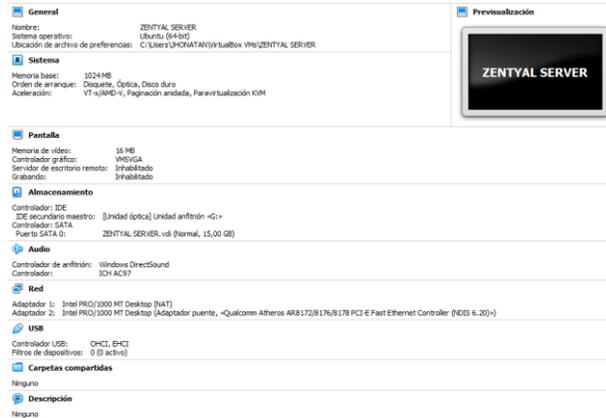


Figura 7.1. Configuración máquina VirtualBox

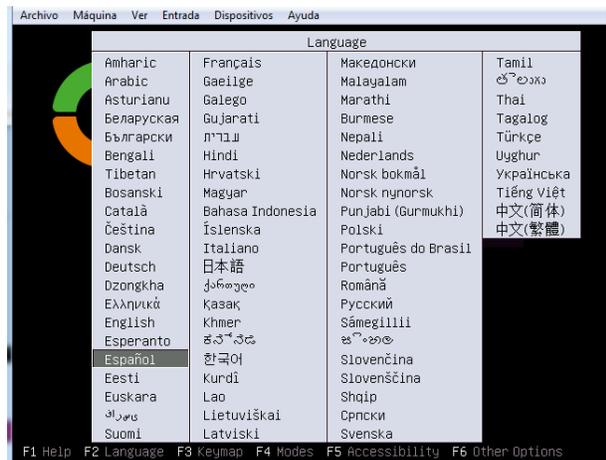


Figura 7.2. Seleccionar el idioma inicial de instalación



Figura 7.3. Seleccionar primera opción del menú de instalación

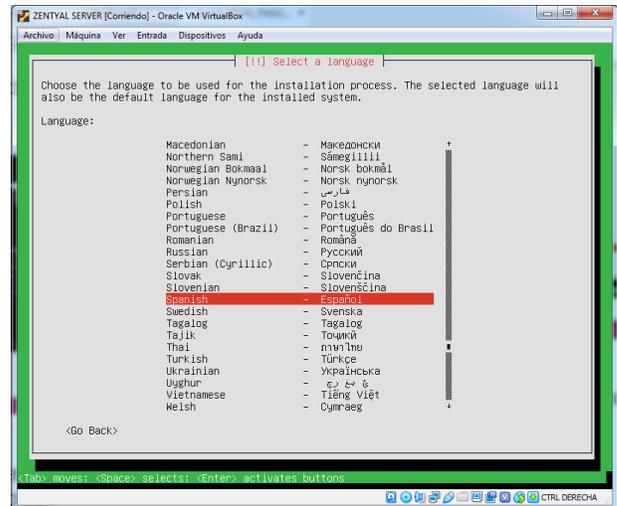


Figura 7.4. Selección del idioma del sistema Zentyal Server



Figura 7.5. Configuración de la interfaz de red primaria

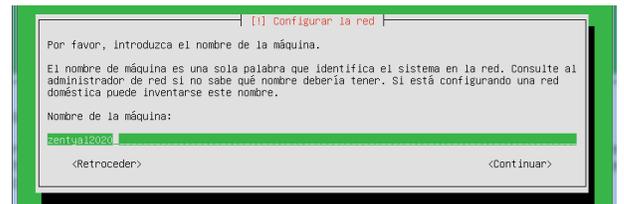


Figura 7.6. Ingresar el nombre de la máquina zentyal2020

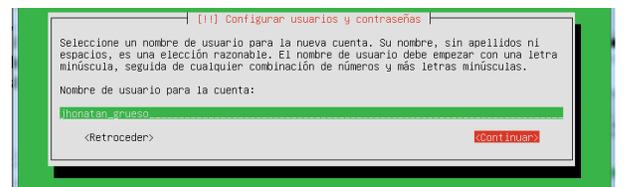


Figura 7.7. Ingresar el nombre de la cuenta de usuario jhonatan_gueso

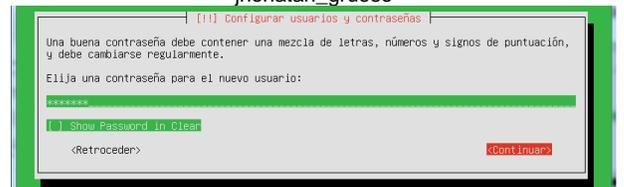


Figura 7.8. Ingresar clave de acceso para el usuario creado



Figura 7.9. Finalización de la instalación



Figura 7.10. Interfaz de inicio luego de la instalación



Figura 7.11. Selección de los paquetes a instalar



Figura 7.12. Estado final de la configuración de Zentyal Server

7.2 CONFIGURACION VPN

Implementación y configuración detallada de la creación de una VPN que permita establecer un túnel privado de comunicación con una estación de trabajo GNU/Linux Debian 10. Se debe evidenciar el ingreso a algún contenido o aplicación de la estación de trabajo.

¿Qué es una VPN?

Una red privada virtual (RPV), en inglés: Virtual Private Network (VPN), es una tecnología de red de computadoras que permite una extensión segura de la red de área local (LAN) sobre una red pública o no controlada como Internet. Permite que la computadora en la red envíe y reciba datos sobre redes compartidas o públicas como si fuera una red privada con toda la funcionalidad, seguridad y políticas de gestión de una red privada. Esto se realiza estableciendo una conexión virtual punto a punto mediante el uso de conexiones dedicadas, cifrado o la combinación de ambos métodos.

Ejemplos comunes son la posibilidad de conectar dos o más sucursales de una empresa utilizando como vínculo Internet, permitir a los miembros del equipo de

soporte técnico la conexión desde su casa al centro de cómputo, o que un usuario pueda acceder a su equipo doméstico desde un sitio remoto, como por ejemplo un hotel. Todo ello utilizando la infraestructura de Internet.

La conexión VPN a través de Internet es técnicamente una unión wide area network (WAN) entre los sitios, pero al usuario le parece como si fuera un enlace privado de allí la designación «virtual private network».

Para comenzar la configuración es importante cerciorarse que dentro de los módulos se encuentre activo el VPN.



Figura 7.13. Activar el módulo VPN

Ahora nos dirigimos a la opción VPN > Servidores y presionamos sobre *módulo de autoridad de certificación*:



Figura 7.14. Acceso a servidores VPN

Ingresamos los datos solicitados en las casillas disponibles.



Figura 7.15. Creación de certificado.

Ahora, de nuevo retornamos a la ruta VPN > Servidores para asignar un nombre al servidor creado, y luego en guardar cambios.

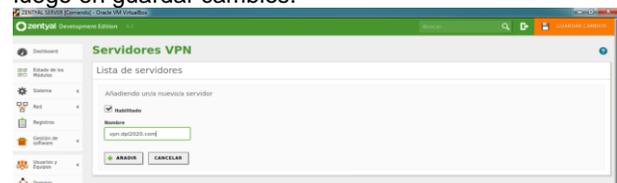


Figura 7.16. Asignar nombre al nuevo servidor

Luego de creado, se selecciona la opción configuración.



Figura 7.17. Configuración del servidor creado

Acto seguido, sería configurar la interfaz donde va a escuchar el DNS, Dominio y el Servidor WINS encontradas en la parte inferior de la ventana, posteriormente presionar sobre la opción cambiar. Es muy importante conocer la IP pública para este caso.

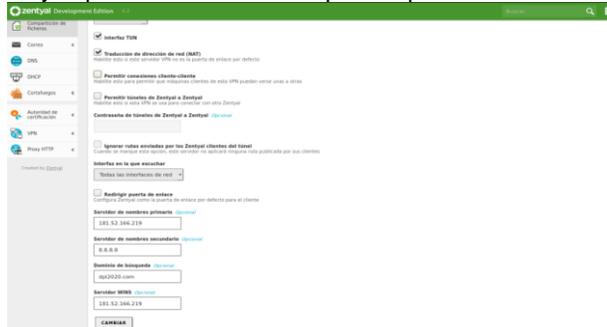


Figura 7.18. Modificación de parámetros

De nuevo, se dirige hacia la opción VPN > Servidores para poder *descargar paquete de configuración de cliente*.



Figura 7.19: Descarga de archivo de configuración para cliente.

Se crea un nuevo certificado para el cliente.



Figura 7.20. Creación de certificado

Procedemos a agregar un nombre al certificado del cliente.

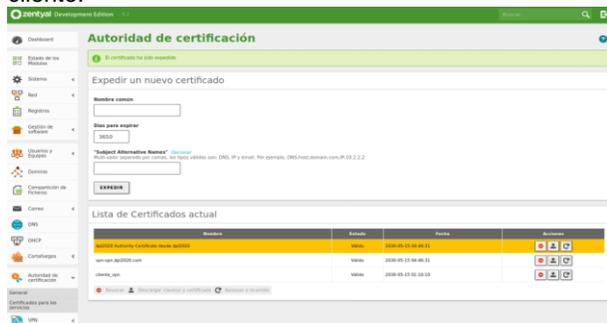


Figura 7.21. Nombre para el certificado del cliente

Creación del servicio de red que permitirá la conexión con el servidor.

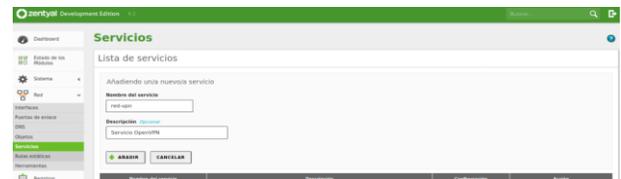


Figura 7.22. Creación del servicio de conexión OpenVPN

Configuración del servicio creado y guardamos cambios.



Figura 7.23. Configuración del servicio de red

Añadimos el servicio creado al cortafuegos, para esto seleccionamos *filtrado de paquetes* y luego en configurar reglas para reglas de filtrado desde las redes internas a Zentyal.



Figura 7.24. Reglas de filtrado

Ahora, se añadirá el servicio creado anteriormente a la regla de configuración.



Figura 7.25. Añadiendo nueva regla de configuración de redes

Una vez creado el certificado, se debe indicar las características para permitir el acceso cliente. Para saber la dirección adicional en la terminal y escribimos IFCONFIG.



Figura 7.26. Nuevos parámetros para el cliente

Una vez realizados los pasos anteriores, se puede observar el estado del servidor VPN habilitado y funcionando.

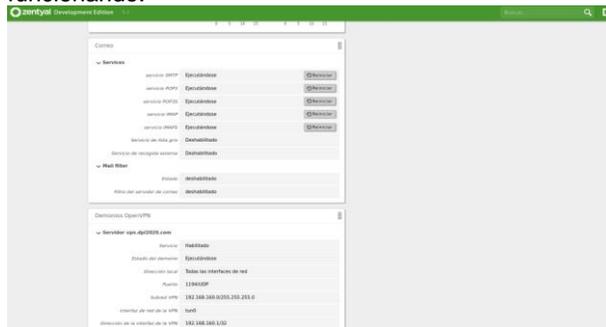


Figura 7.27. Configuración finalizada del VPN

A partir de ahora iniciamos las pruebas de conexión desde el sistema operativo Debian que será nuestro equipo cliente, utilizando el navegador se ingresa la siguiente dirección perteneciente al servidor VPN de Zentyal <https://192.168.1.66:8443/OpenVPN>, y aceptamos el riesgo para ingresar al sitio.

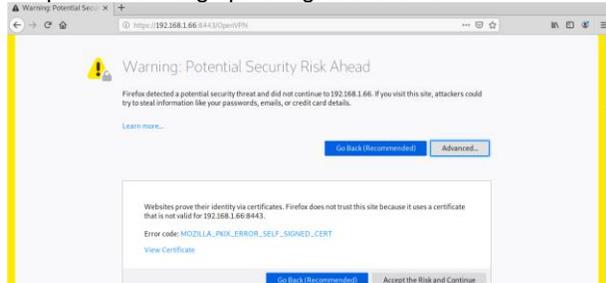


Figura 7.28. Ingresando al VPN de Zentyal Sever

Ya iniciada sesión, se procede a descargar el paquete de configuración del cliente que será en un archivo comprimido.

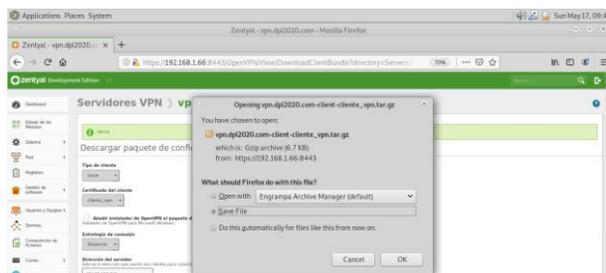


Figura 7.29. Descargando el paquete de configuración cliente

Desde la terminal de Debian se debe descomprimir el archivo descargado en la carpeta `/home/jhonatan/Downloads`.



Figura 7.30. Descomprimiendo paquete de instalación cliente

Verificación o instalación de la aplicación OpenVPN mediante el comando `$sudo apt-get install openvpn`.

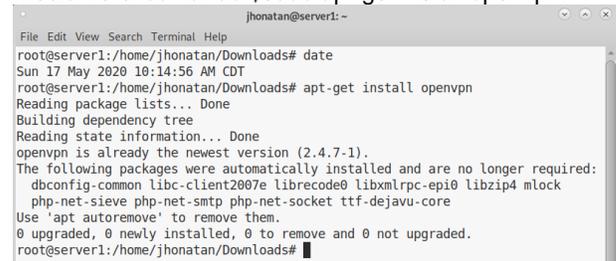


Figura 7.31. Comprobación del estado de OpenVPN

Se continua con la instalación del archivo descomprimido con el nombre de `vpn.dpl2020.com-client.conf`

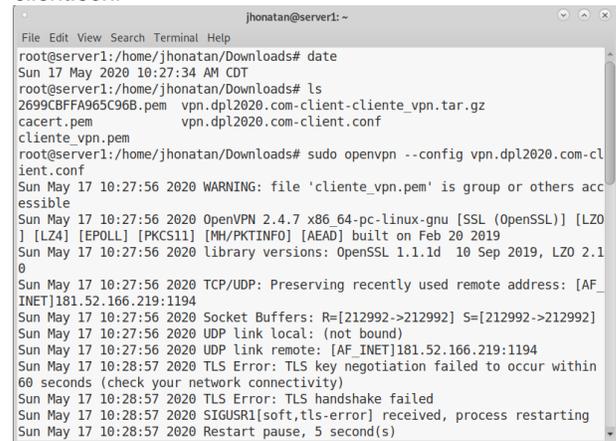


Figura 7.32. instalación del archivo vpn

8 CONCLUSIONES

Una vez colocado en marcha el cortafuegos, presenta una fácil instalación de los diferentes módulos en la parte gráfica, la organización de estos es ubicada en modo intuitivo y de fácil acceso.

En las pautas para la configuración de los servicios, el programa no deja configurar acciones que conllevan una habilitación anterior de otro servicio, en el caso particular de este trabajo se debe habilitar la funcionalidad de DHCP para configurar las reglas de cortafuegos.

Esta distribución presenta la posibilidad de crear objetos y servicios; tanto los objetos como los servicios pueden agrupar varias direcciones o varios servicios en un solo objeto, lo que simplifica y genera una ventaja a la hora de configurar múltiples opciones.

La configuración presenta por otro lado, un lento guardado de los diferentes módulos, cada vez que se configura algún servicio este debe de ser guardado, no se aconseja configurar varios servicios y después aplicar el guardado, ya que puede generar a errores o caídas del programa.

La configuración de una VPN bajo un sistema operativo totalmente desconocido, se ha logrado precisar resultados muy positivos respecto a la capacidad de comprensión y facilidad que ofrece Zentyal server.

Es importante recalcar que a medida que se desarrollaron las diferentes temáticas de esta fase del diplomado, se ha dado a conocer un mundo fascinante en el uso de las diferentes distribuciones de GNU/Linux, que son una excelente alternativa en cuanto costos, seguridad, operatividad y soporte.

9 REFERENCIAS

- [1] «Debian -- El sistema operativo universal». <https://www.debian.org/index.es.html> (accedido may 17, 2020).
- [2] A. Patawari, Getting started with ownCloud: the only precise guide to help you set up and scale ownCloud for personal and commercial usage. Birmingham: Packt Publ, 2013.
- [3] «Inicio», Zentyal Linux Server. <https://zentyal.com/es/inicio/> (accedido may 17, 2020).
- [4] S. Shah y W. Soyinka, Manual de administración de Linux. México: McGraw-Hill, 2010.
- [5] «Zentyal 6.1 Documentación Oficial — Documentación de Zentyal 6.1». <https://doc.zentyal.org/es/> (accedido may 17, 2020).
- [6] Rokitoh. (2016) Instalar servidor de VPN en Zentyal Server 5 Recuperado de <https://red-orbita.com/?p=7680>
- [7] Zentyal Community. (S.F.) Instalación. Recuperado de los documentos Zentyal <https://doc.zentyal.org/es/installation.html>