SOLUCIONANDO NECESIDADES ESPECÍFICAS GNU/LINUX

Luis Fernando González Bermúdez
e-mail: lfgonzalezbe@unadvirtual.edu.co
Johan Sebastian Vargas Vosmediano
e-mail: jvargasvo@unadvirtual.edu.co
Mónica Farley Sánchez Montes
e-mail: mfsanchezmon@unadvirtual.edu.co
Juan Felipe Castillo Cutiva
e-mail: jfcastillocu@unadvirtual.edu.co

RESUMEN: *Se proveen los pases del proceso de instalación y configuración de diferentes servicios para la administración de un entorno de red bajo el servidor Zentyal 6.2 desde su interfaz Web, se iniciará desde la parte básica de implementación del entorno del servidor, se activarán los módulos necesarios que permitirán aplicar la configuración necesaria en las herramientas del software, finalmente a cada proceso se le aplicara pruebas para validar su correcto funcionamiento.*

ABSTRACT: *The steps of the installation and configuration process of different services are provided for the administration of a network environment under the Zentyal 6.2 server from its Web interface, it will start from the basic part of implementation of the server environment, the necessary modules will be activated in order to allow and apply the necessary configuration in the software tools. Finally, each process will be tested to validate its correct operation.*

PALABRAS CLAVE: Seguridad informática, Servicios de red, servicios Web, Zentyal 6.2.

1 INTRODUCCIÓN

Se instala Zentyal Server en una máquina virtual, la cual es gratuita, de código abierto y está basado en Ubuntu; es ideal para las pequeñas y medianas empresas que quieren adoptar un servidor para sus redes que preste servicios como correo, DNS, DHCP implementando controlador de dominio desde una máquina virtual, Proxy desde un equipo servidor para un equipo cliente, aplicando diferentes procesos que permite la comunicación entre los dispositivos y su respectiva función para restringir el ingreso a los sitios web, Firewall teniendo a disposición varios servicios de Infraestructura para poder acceder a nuestra red, siendo compatible también con servicios que prestan los sistemas Windows.

Esto con el fin de tener el conocimiento al momento de trabajar en grupos donde se requieran estos procesos dependiendo el tipo de usuarios y lugar donde se aplique, para mantener cierto control en la red y establecer determinados procesos que garanticen un correcto funcionamiento en el servicio.

2 INSTALACIÓN ZENTYAL 6.2

2.1 CARACTERÍSTICAS GENERALES

Se ingresa a la página principal de Zentyal https://zentyal.com/community/ y en la parte inferior de la página web podremos encontrar las diferentes versiones del sistema operativo, para el caso se descargará la versión 6.2

2.2 CONFIGURACIÓN DE LA MÁQUINA VIRTUAL

Se procede a crear la maquina con las siguientes características:

- Tamaño de memoria: 2048
- Disco duro: Crear un disco duro virtual ahora
- Tipo de archivo de disco duro: VDI (VirtualBox Disk Image)
- Almacenamiento en unidad de disco dura física: Reservado dinámicamente
- Ubicación del archivo y tamaño: 40 GB

2.3 PROCESO DE INSTALACIÓN

El proceso de instalación es similar al que se lleva a cabo para instalar Ubuntu desktop.

Se elige el lenguaje que usará el sistema operativo, una ubicación geográfica, la configuración del teclado, el adaptador de red principal, el nombre del servidor, el nombre del administrador que tendrá privilegios de root, la contraseña del administrador y la confirmación de esta que también sirven para las conexiones por SSH y la ubicación geográfica. Terminados estos pasos se inicia el proceso instalación que puede tardar hasta 20 minutos.

Una vez terminado el proceso de instalación, se debe retirar la imagen de la unidad óptica y reiniciar el sistema operativo.

Luego de reiniciar el sistema se abre el navegador, se aplica la excepción de seguridad para visualizar el panel de control del Zentyal, a continuación, se ingresa el nombre de usuario y contraseña y se ingresa la licencia para su activación y visualizar el panel

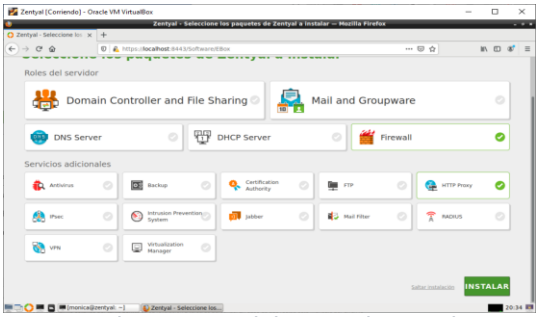

Figura 1:Panel de control Zentyal 6.2

3 ACTIVIDADES A DESARROLLAR

3.1 TEMÁTICA 1: DHCP SERVER, DNS SERVER Y CONTROLADOR DE DOMINIO

3.1.1 DHCP SERVER.

Una vez instalado Zentyal se inicia configurando el estado de los módulos:

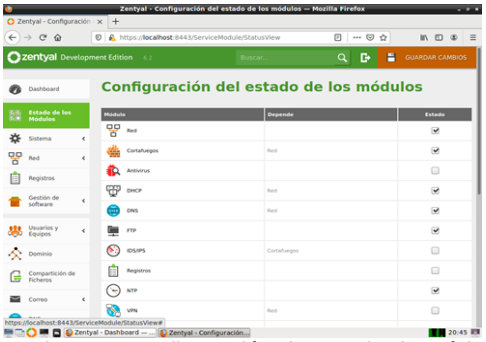

Figura 2:Configuración de estado de módulos

Desde el panel del servidor en la parte izquierda se pueden apreciar todos los módulos instalados, se elige DHCP y se selecciona el apartado de configuración de la interfaz de red interna denominado eth1:

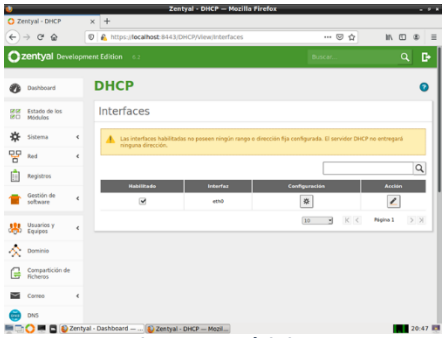

Figura 3: Módulo DHCP

Se da clic en configuración y se configuran las interfaces interna y externa, catalogadas con eth0 con la etiqueta Lan – Red Local y eth1 con la etiqueta Wan – Externa:

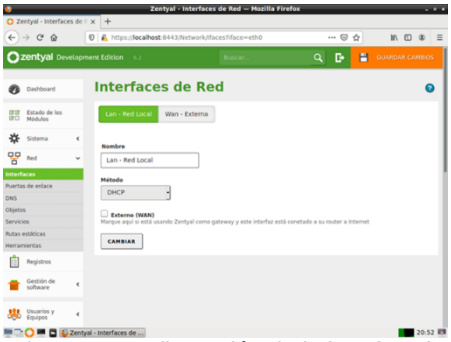

Figura 4: Configuración de la interface interna

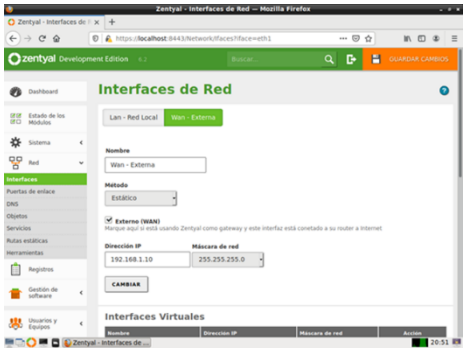

Figura 5: Configuración de la interface externa

Para asignar direcciones dinámicamente a las maquina cliente se elige un rango de red:

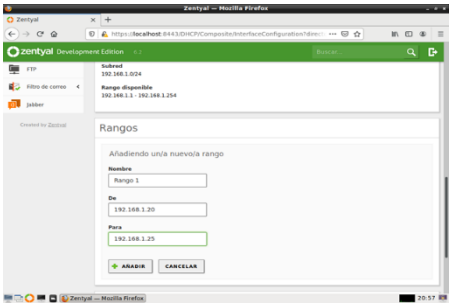

Figura 6:Asignación de rango DHCP.

Se constata la asignación de IP al cliente aparece en el Dashboard con la dirección 192.168.1.20:

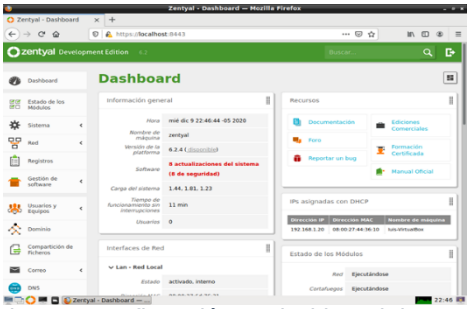

Figura 7:Confirmación en dashboard de Zentyal de asignación de IP mediante DHCP.

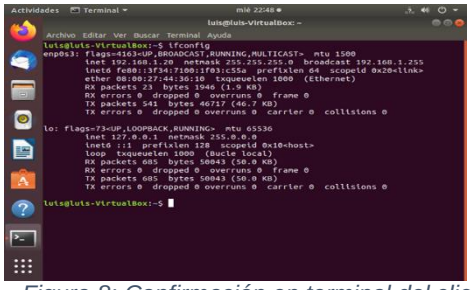

Figura 8: Confirmación en terminal del cliente Ubuntu de asignación de IP 192.168.1.20 mediante DHCP.

3.1.2 DNS SERVER

Para que la maquina cliente pueda entender direcciones de internet debe habilitar el servicio o modulo DNS desde el panel de configuración del servidor Zentyal y guardando los cambios:

Figura 9:Confirmación de activación del módulo DNS

Se confirma que el nombre de servidor primario sea el DNS local del servidor Zentyal y se procede a confirmar el cambio y guardando esta configuración:

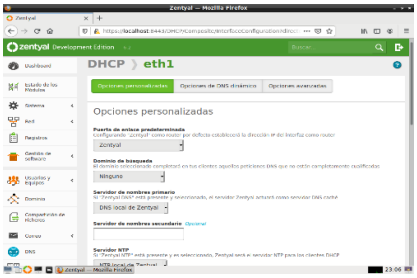

Figura 10:Confirmación de servidor primario

Ahora en DNS se procede al apartado de configuración de las direcciones IP del dominio, se da clic en direcciones IP del dominio:

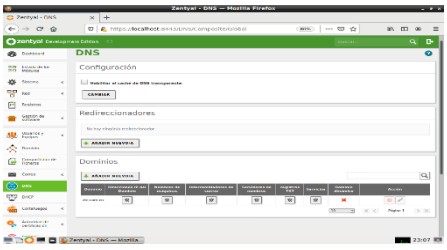

Figura 11:Interfaz de configuración de DNS.

Ahora se añade la dirección IP de la maquina cliente y de todos los demás clientes conectados al servidor Zentyal y se guardan los cambios.

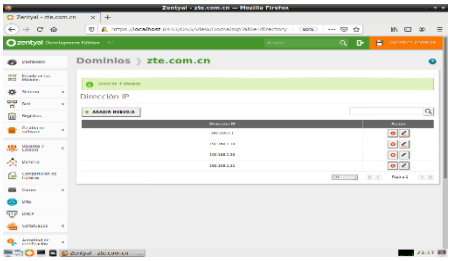

Figura 12:Adición de direcciones IP de clientes.

Para confirmar que el paso anterior tuvo efecto en la maquina cliente se cambia hacia la maquina cliente, y en el apartado de configuración de la red se puede apreciar la dirección IP asignada y los respectivos DNS:

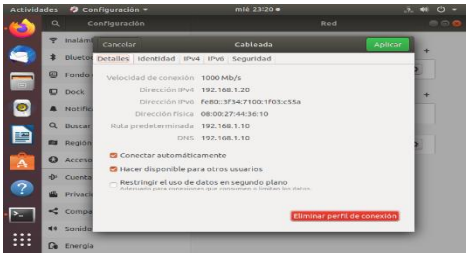

Figura 13: Confirmación de asignación de la IP del servidor Zentyal a la configuración del cliente

3.1.3 Controlador de Dominio.

Se va a la sección de dominios para crear los registros DNS:

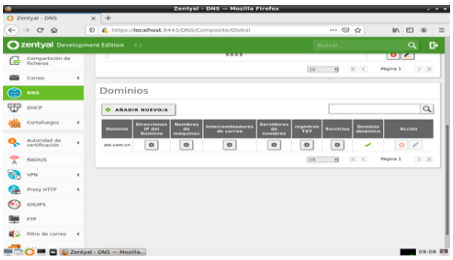

Figura 14:Interfaz de Dominios

Se da clic en Nombres de máquinas y se añade la máquina cliente y su dirección ip:

Figura 15: Adición de nombre de máquina Luis-VirtualBox

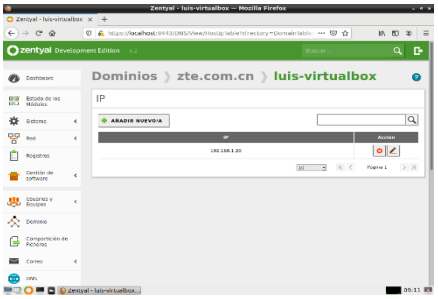

Figura 16:Adición de dirección ip del cliente.

En Dominio se observa que este configurado como controladora de dominio y se activa perfiles móviles:

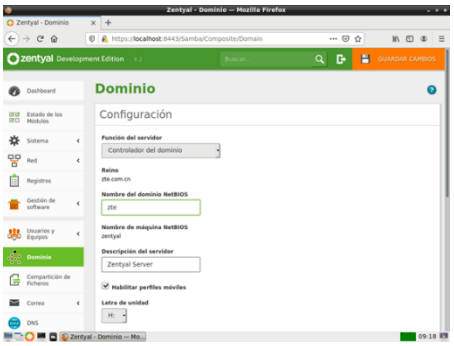

Figura 17:Configuración de controladora de dominio.

Se crean 2 usuarios:

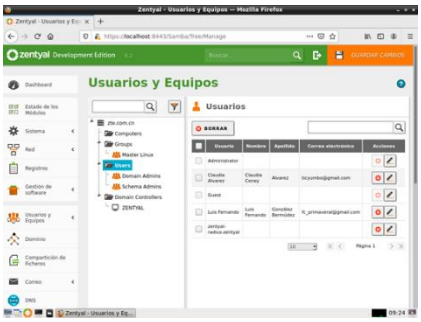

Figura 18:Creación de 2 usuarios

Se ingresa a reglas de cortafuegos. Se crea una nueva regla de filtrado desde redes externas a Zentyal

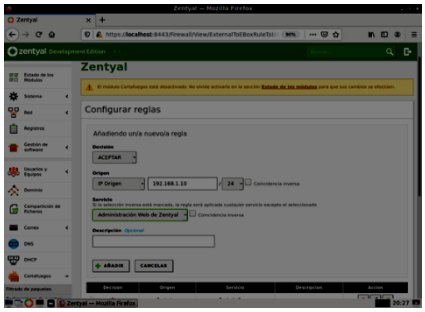

Figura 19:Creación de nueva regla de filtrado desde redes externas.

Se regresa a estado de módulos y se activa el corta fuegos

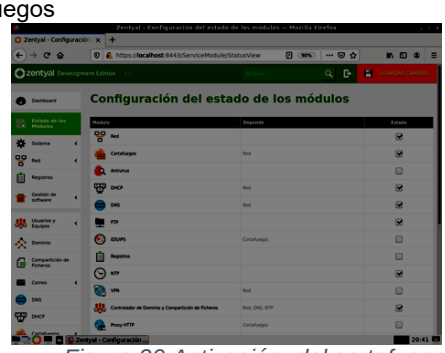

Figura 20:Activación del cortafuego

Se comprueba la efectiva conexión a Internet

Figura 21:Conexión a internet.

Se hace ping a la dirección de Zentyal 192.168.1.10 desde el cliente:

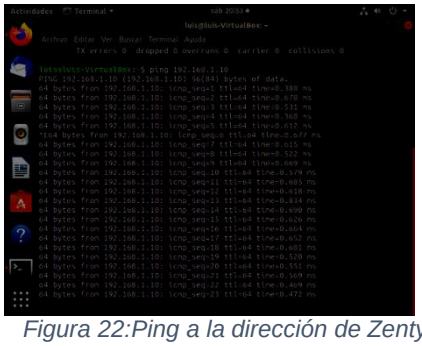

Figura 22:Ping a la dirección de Zentyal.

3.2 TEMÁTICA 2: PROXY NO TRANSPARENTE

Implementación y configuración detallada del 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.

Para esto debemos instalar el componente HTTP Proxy, y cortafuegos para ello vamos al panel de la izquierda, Software Componentes de Zentyal y allí veremos la lista de componentes disponibles.

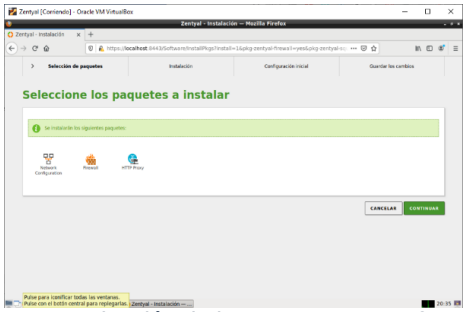

Figura 23:Selección de los paquetes Cortafuegos y Proxy HTTP

Instalamos los componentes y se observan a la izquierda

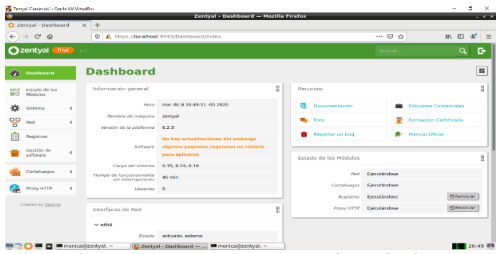

Figura 24: Componentes instalados

Se configura las interfaces de red desde virtualbox que permiten la comunicación de los equipos, ingresar a configuración del equipo Zentyal, seleccionar la opción red, seleccionar la interfaz1 conectado NAT, interfaz 2 conectado Red Interna DMZ.

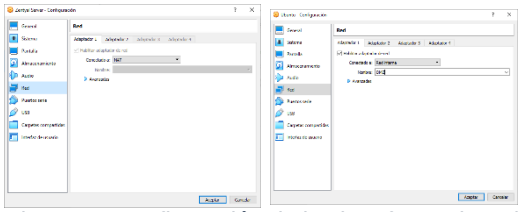

Figura 25:Configuración de las interfaces de red

Se selecciona la configuración de las tarjetas de red o interfaces de la máquina. En este caso la eth0 es la externa que nos provee internet y la eth1 la interna.

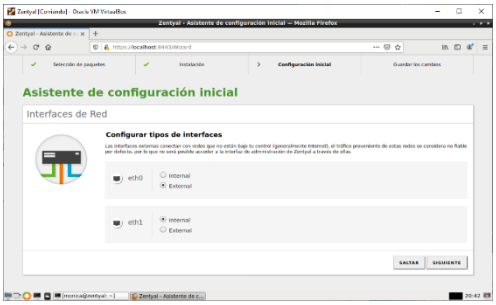

Figura 26:Configuración de las tarjetas de red en Zentyal

Se crea el perfil de filtrado

Figura 27:Pefil de filtrado

Se configuran las reglas de filtrado

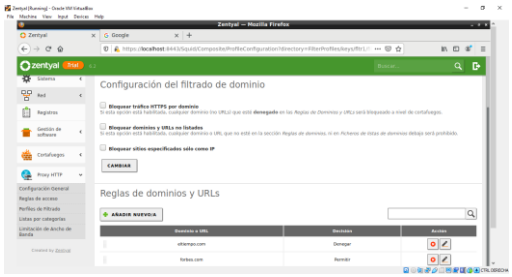

Figura 28:Reglas de filtrado

Ahora se ingresa el submenú Reglas de acceso ubicado como un submenú del módulo Proxy HTTP, y se adiciona el perfil que se creó: diplomadolinux

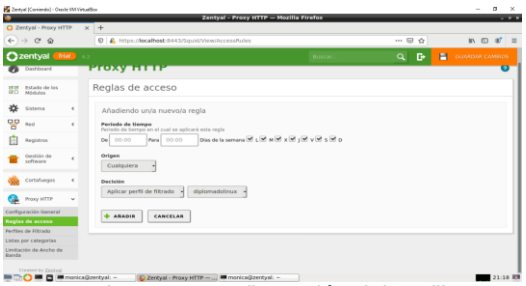

Figura 29:Configuración del perfil

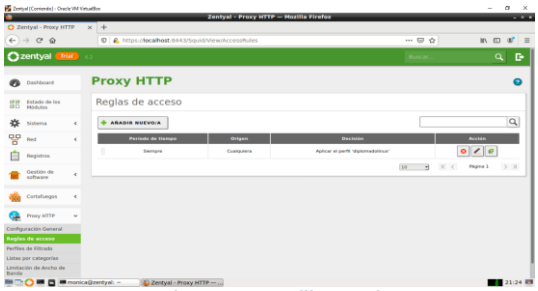

Figura 30:Pefil creado

Se configura el puerto 1230 del proxy

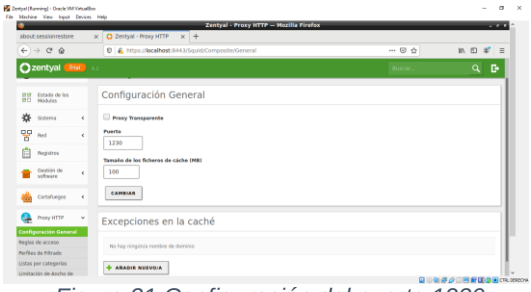

Figura 31:Configuración del puerto 1230

Se ingresa a la máquina cliente Ubuntu y se configura ip y la puerta de enlace configurada en el Zentyal para la interface (eth1), ingresando con sudo nano /etc/network/interfaces

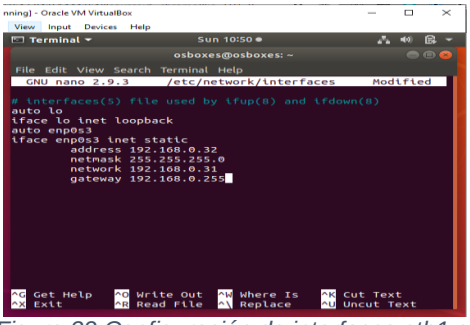

Figura 32:Configuración de interfaces eth1 en cliente

Se prueba la conexión

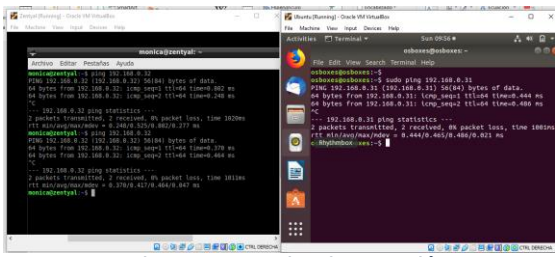

Figura 33:Prueba de conexión

Ahora se ingresa a la máquina Ubuntu y se configura los puertos para HTTP y HTTPS.

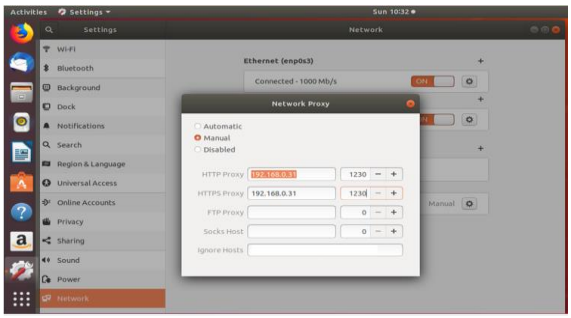

Figura 34:Configuración de puertos en cliente

Se ingresa a internet

Figura 35:Prueba de acceso a internet en el cliente

Se ingresa a la página del Forbes que se configuró en las reglas de acceso

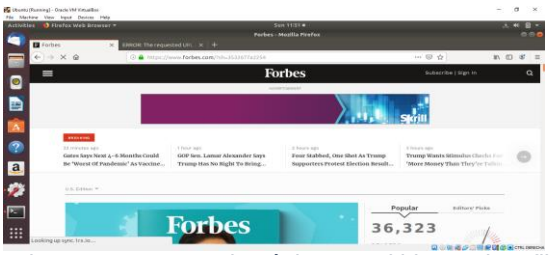

Figura 36:Ingreso a la página permitida en el perfil

Se ingresa a la página del Tiempo con reglas denegada.

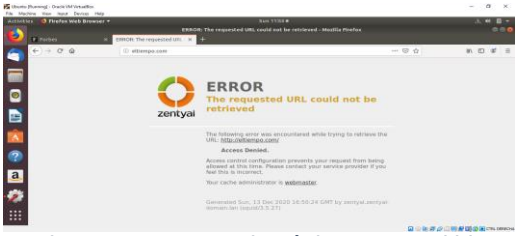

Figura 37:Ingreso a la página no permitida en el perfil

3.3 TEMÁTICA 3: CORTAFUEGOS

Estando dentro de la sub-pestaña de Filtrado de Paquetes, aparecen cuatro tipos de reglas para configurar el firewall. Seleccionamos Reglas de filtrado para las redes internas.

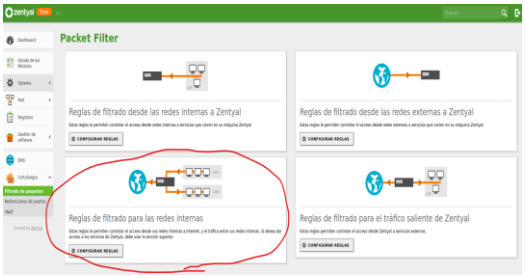

Figura 38: Selección de Reglas de filtrado para las redes internas.

Antes de crear cualquier regla en el Firewall, hay una que viene creada por defecto la cual permite el tráfico desde y hasta cualquier IP sin importar que tipo de servicio sea. Es recomendable eliminar esta regla por defecto. Luego damos clic en el botón Añadir Nuevo para crear una nueva regla.

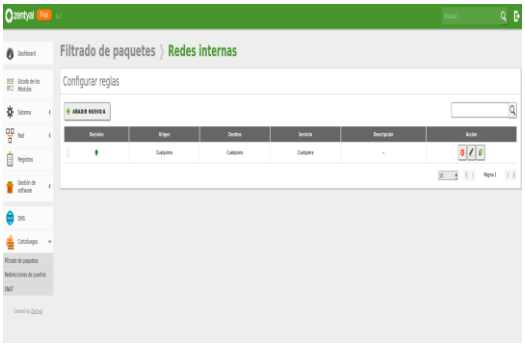

Figura 39: Reglas de Redes internas por defecto.

La información a rellenar dentro de los campos para crear la nueva regla son la decisión, si es Aceptar, Denegar o Registrar. La IP Origen que es de donde se genera el tráfico y la IP Destino que es a donde se dirige el tráfico en la red. También un cuarto campo que nos pide el tipo de servicio, por qué protocolo se estará configurando la nueva regla y una descripción general de la regla.

Figura 40: Añadir nueva regla.

Antes de continuar configurando las reglas, es necesario percatarnos de que todas las páginas web de entretenimiento y redes sociales se encuentran habilitadas en la estación de trabajo GNU/Linux antes de activarlas. Por ello, procedemos a inicializar nuestra máquina virtual donde tenemos instalado Linux Ubuntu 20.04 64 Bits.

Facebook se encuentra habilitado.

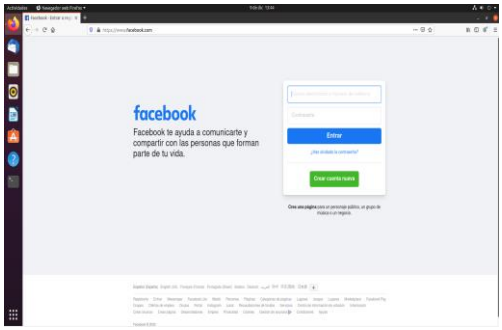

Figura 41: Ingreso a página www.facebook.com.

Instagram se encuentra habilitado.

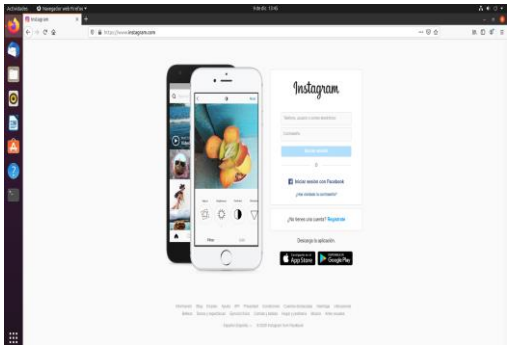

Figura 42:Ingreso a página www.instagram.com.

Spotify se encuentra habilitado.

Figura 43:Ingreso a página www.spotify.com.

WhatsApp Web se encuentra habilitado.

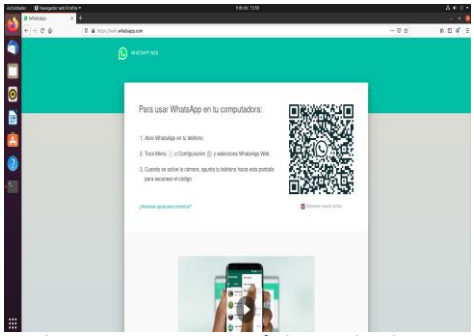

Figura 44:Ingreso a página web.whatsapp.com.

Con la prueba de que los sitios web están habilitados, ahora procederemos a tomar su dirección IP, esto lo hacemos por medio de la consola haciendo PING a la dirección DNS de cada dominio.

Figura 45:Comando ping a dirección www.facebook.com.

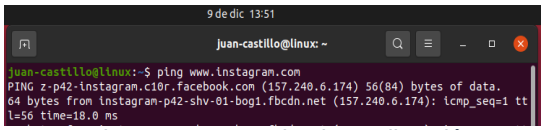

Figura 46:Comando ping a dirección www.instagram.com.

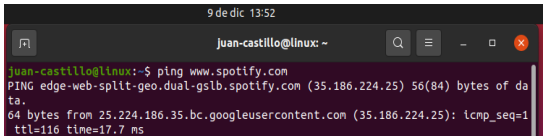

Figura 47:Comando ping a dirección www.spotify.com.

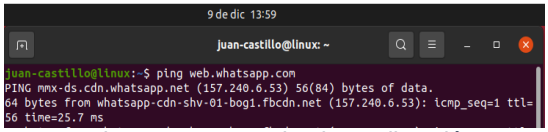

Figura 48:Comando ping a dirección web.whatsapp.com.

Con las IP de todos los sitios web procedemos a crear las reglas con su respectiva decisión de denegar el tráfico a esa IP Destino desde cualquier IP Origen.

Figura 49:Configuración de reglas.

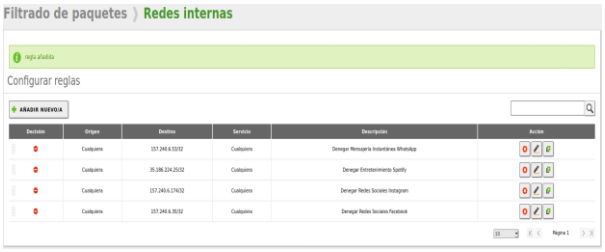

Figura 50:Reglas creadas.

Solo nos resta Guardar los cambios realizados. Con el servicio de Firewall configurado completamente y bloqueando las páginas web requeridas, procedemos a configurar por último el direccionamiento IPv4 de la estación de trabajo GNU/Linux, donde asignaremos una IP estática que se encuentre dentro del segmento de Zentyal Server como lo puede ser 150.12.0.10 ya que la dirección IP del servidor Zentyal Server quedo configurada como 150.12.0.2 sería la puerta de enlace de la estación de trabajo GNU/Linux.

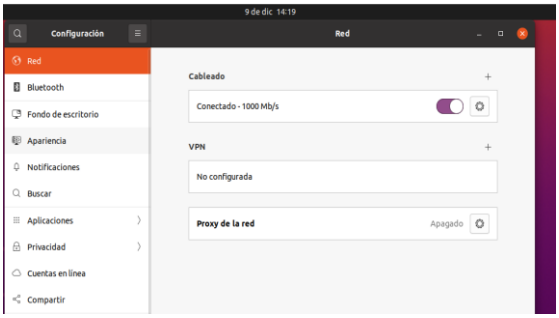

Figura 51:Configuración de red.

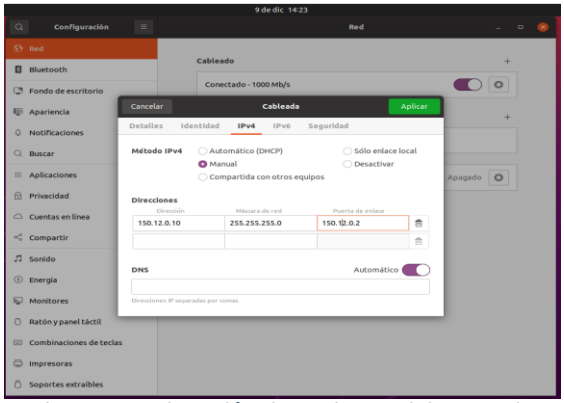

Figura 52:Asignación de IP dentro del rango de Zentyal.

Realizamos la prueba de ingreso a las mismas páginas anteriormente ingresadas.

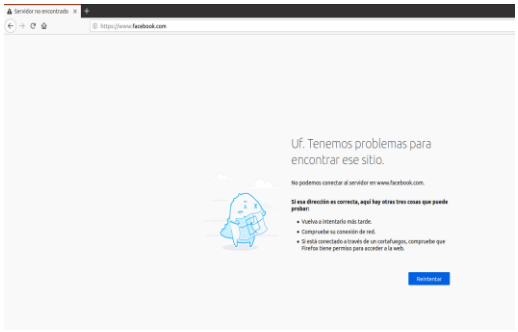

Figura 53:Ingreso denegado a www.facebook.com.

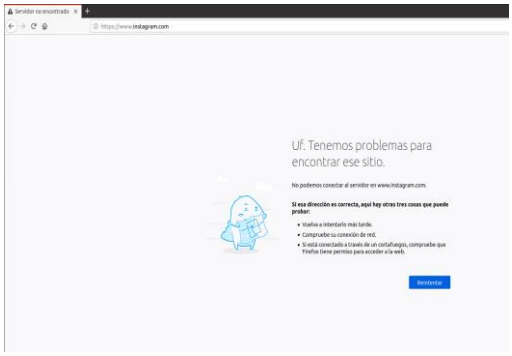

Figura 54:Ingreso denegado a www.instagram.com.

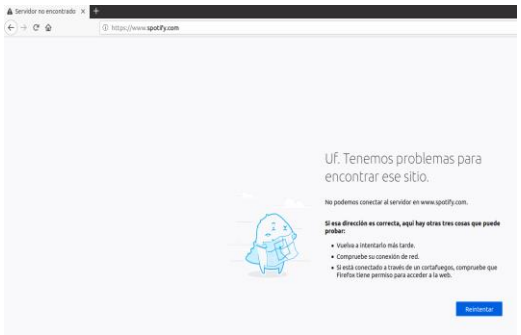

Figura 55:Ingreso denegado a www.spotify.com.

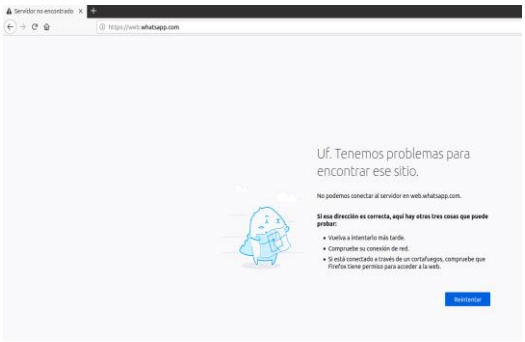

Figura 56:Ingreso denegado a web.whatsapp.com.

Como podemos observar, las direcciones de entretenimiento y redes sociales mencionadas anteriormente se han vuelto inaccesibles al tratar de cargarlas.

3.4 TEMÁTICA 4: FILE SERVER Y PRINT SERVER

3.5 TEMÁTICA 5: VPN

Una red privada virtual (RPV), en inglés: Virtual Private Network (VPN), es una tecnología de red de ordenadores que permite una extensión segura de la red de área local (LAN) sobre una red pública o no controlada como Internet. Permite que el ordenador 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.

Se puede configurar Zentyal para dar soporte a clientes remotos, a través del servicio VPN, ya que un servidor Zentyal, trabaja como puerta de enlace y como servidor VPN, que tiene una red local detrás, permitiendo a clientes externos conectarse a dicha red local.

Para este punto, manejan dos máquinas virtuales, una para el servidor Zentyal y otra para la maquina cliente con el sistema operativo Ubuntu Desktop. Ambas maquinas tienen dos adaptadores uno en Bridge y el otro en Red Interna.

3.5.1 CONFIGURACIÓN DE SERVIDOR VPN

Después de instalar el servidor y los paquetes necesarios que son Cortafuegos o Firewall, Autoridad de certificado y VPN, se configuran las dos interfaces del servidor (eth0 y eth1), para este punto estas se manejaron eth0 como externa y eth1 como interna y ambos con IP dinámica es decir DHCP.

Una vez realizada la configuración anterior, lo primero que se realiza es generar el certificado de autenticidad del servidor Zentyal, esto se realiza en el Menú “Autoridad de Certificación” en la sección “General”.

En el formulario se debe ingresar el nombre con el cual aparecerá el certificado y, además, el tiempo de vigencia que este tendrá

Figura 57:Certificado de autenticidad

Una vez creado el certificado, procederemos a crear o generar, el servidor VPN, para ello se debe ir al Menú "VPN" y a la sección "Servidores". Se añade un nuevo servidor el cual por ahora debe estar inhabilitado.

Figura 58:Generar servidor VPN

Una vez generado el servidor VPN, se debe generar el certificado de este. Para ello se regresa al menú "Autoridad de certificados a la sección "General" y se llena la información.

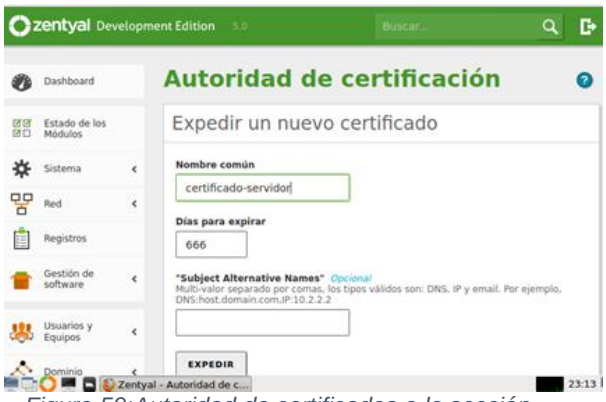

Figura 59:Autoridad de certificados a la sección

Una vez generado el certificado, se debe configurar el servidor VPN. Para esto nos vamos al menú "VPN" a la sección "Servidores" y se accede a la configuración del servidor VPN. En este punto se define el puerto del servidor el cual es UDP y se deja el túnel por defecto. Se deja la dirección VPN que está por defecto, aunque si se desea se puede cambiar; se selecciona el certificado del servidor recién generado y se habilita la interfaz TUN.

Figura 60:Interfaz TUN

3.5.2 CREACIÓN DEL SERVICIO VPN

Una vez se tenga el servidor VPN configurado, se debe generar el servicio que funciona con el servidor. Para esto vamos al menú "Red" y a la sección "Servicios". Allí se genera un nuevo servicio.

Figura 61:Nuevo servicio VPN

Tras añadir el servicio, se debe configurar; para ello se accede a la configuración del servicio creado, se agrega un nuevo perfil de configuración y se ingresa la misma información del puerto del servidor VPN creado, en donde el puerto de origen puede ser cualquiera y el puerto de destino es el mismo del servidor VPN.

Figura 62:Puertos del servidor VPN

3.5.3 ESTABLECIMIENTO DE LA REGLA DE FIREWALL

Con el servicio ya configurado, se debe ahora establecer la regla en el Firewall que permitirá la conexión con el servidor a través del servicio generado. Para ello se accede al menú “Cortafuegos” a la sección “Filtrado de paquetes”. Aquí se debe acceder a la opción “Configurar Reglas” de la sección “Reglas de filtrado desde las redes internas a Zentyal”. Allí se debe indicar que la decisión es de aceptación desde cualquier origen y usando el servicio VPN generado.

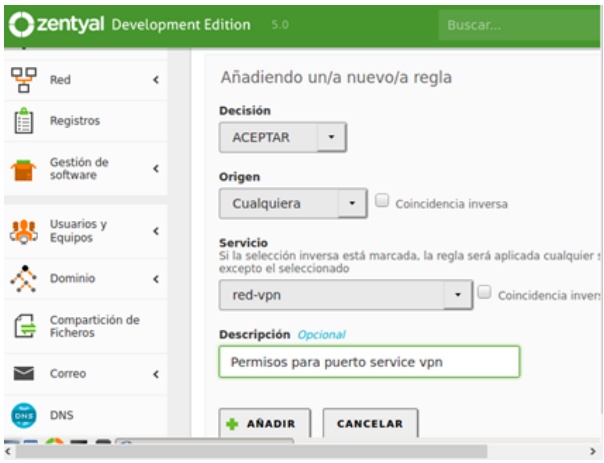

Figura 63:Reglas de filtrado para VPN

Una vez realizado el paso anterior, se retorna al servidor VPN y se accede a la configuración de redes anunciadas. Aquí se debe agregar una nueva red anunciada cuyo nombre puede ser cualquiera.

Figura 64:Red anunciada

3.5.4 PAQUETE DE CONFIGURACIÓN DE CLIENTE

Una vez se genera la lista de redes, se debe descargar el paquete de configuración que usará el cliente. Para ello se accede a la opción en la lista de servidores, en donde se sigue la configuración que está en la imagen, pero se debe obtener la IP pública y la IP local para ingresarlas en el formulario, además de indicar el certificado del cliente del servidor y el tipo del sistema operativo del cliente.

Figura 65:Paquete de configuración cliente

Este paquete se debe enviar a la máquina del cliente. Con el paquete generado se habilita el servidor VPN y se verifica su funcionamiento desde el Dashboard.

Figura 66:Verificación del paquete

3.5.5 CONEXIÓN CLIENTE-SERVIDOR

Tras configurar Zentyal, se debe ir a la máquina del cliente. Una vez allí se descarga y se descomprime el paquete del cliente generado por el servidor. Posteriormente se debe instalar OpenVPN en la máquina.

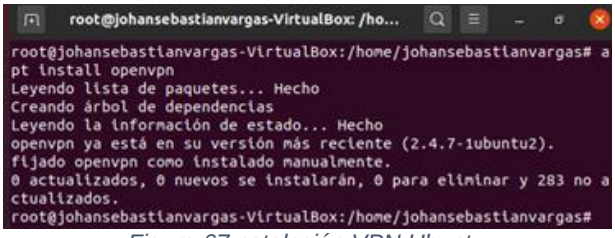

Figura 67:nstalación VPN Ubuntu

Tras instalarlo, ya se puede realizar la conexión utilizando el comando *openvpn --config* e indicando la ruta del archivo *.conf* del paquete de configuración.

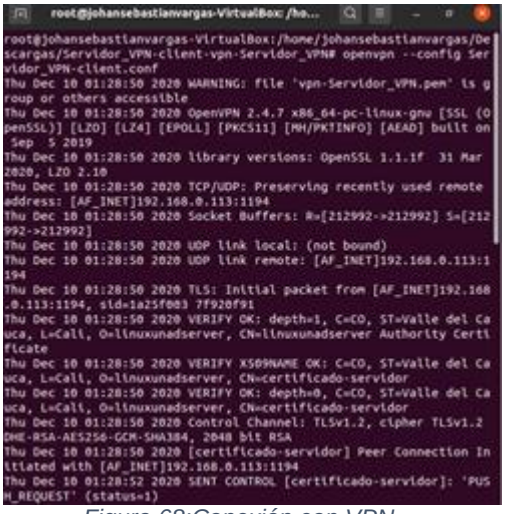

Figura 68:Conexión con VPN

De esta manera se establece la conexión VPN entre el servidor y la máquina Ubuntu. Comprobamos la conexión desde los registros del servidor, se pueden ver las conexiones del servicio VPN y allí debe visualizarse la IP de la máquina Ubuntu.

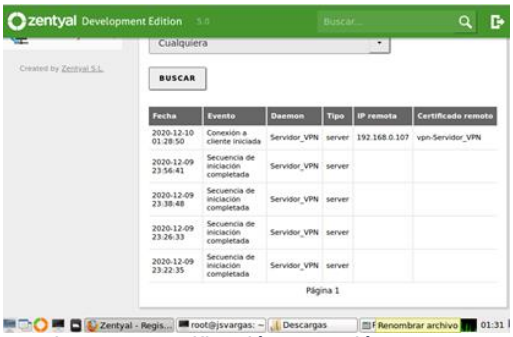

Figura 69: Verificación Conexión VPN

4 CONCLUSIONES

- Se instaló Zentyal Server como sistema operativo en una máquina virtual.
- Se abordó la solución mediante DHCP Server, DNS Server y Controlador de Dominio.
- Se abarcó la implementación y configuración detallada del control del acceso de una estación GNU/Linux a los servicios de conectividad a Internet desde Zentyal a través de un proxy que filtra la salida por medio del puerto 1230.
- Se implementó y configuró detalladamente para la restricción de la apertura de sitios o portales Web de entretenimiento y redes sociales, evidenciando las reglas y políticas creadas. La validación del Funcionamiento del cortafuego aplicando las restricciones solicitadas, se hará desde una estación de trabajo GNU/Linux.
- Se ilustró la 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. Se debe evidenciar el ingreso a algún contenido o aplicación de la estación de trabajo.

5 REFERENCIAS

CeroWarnings CW, 2020. [online] Youtube.com. Available at: https://www.youtube.com/watch?v=3Lr5JU86xcc

CeroWarnings CW, 2020. [online] Youtu.be. Available at: https://youtu.be/V-j4cfTTsmw

Expertos de Computadoras, 2020. [online] Youtube.com. Available at: https://www.youtube.com/watch?v=7RzRVjZJv88&t=8s

itsMoreno YT, 2020. [online] Youtube.com. Available at: https://www.youtube.com/watch?v=ox3gk837dds

JGAITPro, 2020. [online] Youtube.com. Available at: https://www.youtube.com/watch?v=npZauKzGpkY

JGAITPro, 2020. [online] Youtube.com. Available at: https://www.youtube.com/watch?v=H5lhAKOH5LM

Manuel Cabrera Caballero, 2020. [online] Available at: http://biblioteca.udenar.edu.co:8085/atenea/biblioteca/89737.pdf

Santiago Vicente, 2020. [online] Youtu.be. Available at: https://youtu.be/zz6UvEb2e7c

drivemeca. (s.f.). https://drivemeca.blogspot.com/. Obtenido de https://drivemeca.blogspot.com/2018/04/como-instalar-zentyal-server-paso-paso.html

J.Pomeyrol. (30 de Octubre de 2018). Muy Linux. Obtenido de https://www.muylinux.com/2018/10/30/zentyal-linux-small-business-server/

jjvelasco. (6 de Octubre de 2010). Hipertextual. Obtenido de https://hipertextual.com/archivo/2010/10/zentyal-el-servidor-integral-para-pymes/

ragasys. (20 de Marzo de 2019). Ragasys Sistemas. Obtenido de https://blog.ragasys.es/agregar-ubuntu-18-04-lts-a-dominio-active-directory-windows

Zentyal Wiki, «Instalación,» 2017. [En línea]. Available: https://wiki.zentyal.org/wiki/Es/5.0/Instalacion#el-instalador-de-zentyal.

Zentyal Wiki, «Usuarios, Equipos y Comparticion de ficheros,» 2018. [En línea]. Available: https://wiki.zentyal.org/wiki/Es/5.0/Usuarios,_Equipos_y_Compartición_de_ficheros.

C. M, «How to Install and Configure OpenVPN Server on Zentyal 3.4 PDC – Part 12.,» TecMint, 2014. [En línea]. Available: https://www.tecmint.com/install-openvpn-server-on-zentyal/. [Último acceso: 5 12 2019].

Z. Wiki, «Servicio de redes privadas virtuales (VPN) con OpenVPN.,» Zentyal Wiki, [En línea]. Available: https://wiki.zentyal.org/wiki/Es/3.5/Servicio_de_redes_privadas_virtuales_%28VPN%29_con_OpenVPN. [Último acceso: 2 12 2019].