

PASO 8 - SOLUCIONANDO NECESIDADES ESPECÍFICAS CON GNU/LINUX

Edisson Leonardo Ortiz Lozano
elortizlo@unadvirtual.edu.co
Luz Ximena Ríos Rojas
lxriosr@unadvirtual.edu.co
Yiris Griceldis Rangel Torrecilla
ygrangelt@unadvirtual.edu.co

RESUMEN: *En el presente documento se desarrollará la implementación de soluciones tecnológicas TIC, para red de computadores, basados en la distribución Zentyal Server 6.2. Esta distribución es una alternativa, en modo de ejecución gráfica, a los tradicionales servidores GNU/Linux y Windows Server de una infraestructura de red de telecomunicaciones.*

PALABRAS CLAVE: Adaptador puente, GNU/Linux, Ubuntu, Zentyal Server, Proxy, Puerta de enlace.

1 INTRODUCCIÓN

El siguiente trabajo contiene el desarrollo práctico solucionando necesidades específicas con GNU/Linux por medio de la distribución Zentyal Server 6.2, con la configuración de DHCP Server, DNS Server y Controlador de Dominio, Proxy no transparente, Cortafuegos, File Server, Print Server y VPN.

2 INSTALACION ZENTYAL SERVER 6.2

Zentyal Server 6.2 está basado en Ubuntu server, su instalación es similar a dicha distribución y funciona sobre arquitecturas estándar x86 (32-bit) o x86_64 (64-bit). Los requerimientos de hardware para un servidor Zentyal, dependen de los módulos que se instalen dependiendo de cuántos usuarios utilizan los servicios y de sus hábitos de uso. Con el fin de tener una instalación correcta, se debe seleccionar el tipo de red puente, para poder conectarse a las demás máquinas que estén disponibles en la red.

Para la instalación en el primer paso, se procede con la creación de la máquina virtual, donde se le asigna el tamaño de la memoria RAM y disco.

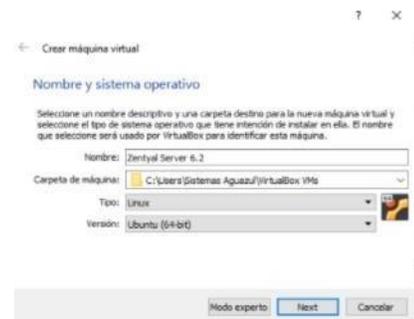


Imagen 1 - Creación máquina virtual.

En configuración, se selecciona almacenamiento, atributos y en unidad óptica se carga la ISO de Zentyal 6.2, para que se identifique como punto de arranque de la máquina virtual.

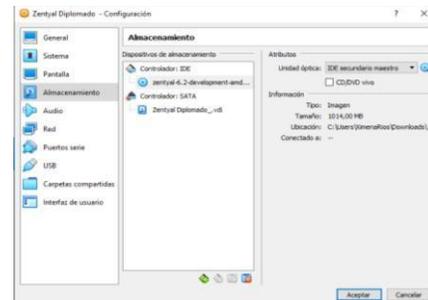


Imagen 2 - Selección ISO Zentyal.

Seguido se configuran las tarjetas de red, donde el primer adaptador es puente y el segundo adaptador es red interna.

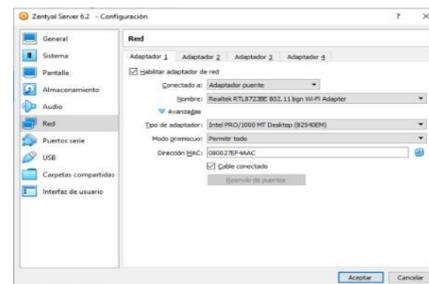


Imagen 3 - Asignación Adaptadores de red.

Se visualiza los cambios realizados en la máquina y se selecciona iniciar.

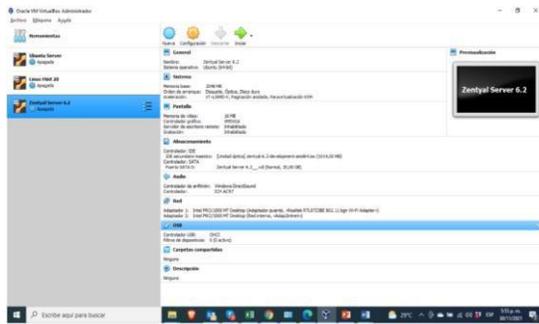


Imagen 4 - Información de la máquina de Zentyal.

Después se elige el idioma para el servidor.



Imagen 5 - Selección de idioma.

Seguido se visualizan las opciones de inicio, donde se selecciona Instalar Zentyal 6.2 (Borrar todo el disco).

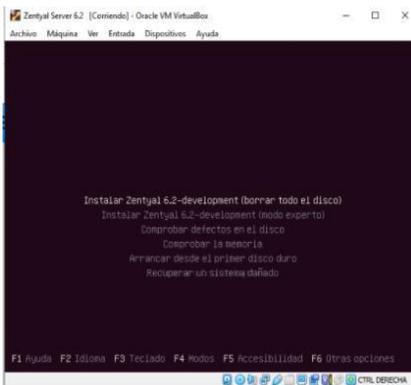


Imagen 6 - Selección Instalar Zentyal 6.2.

Se procede a seleccionar el país de ubicación del usuario.

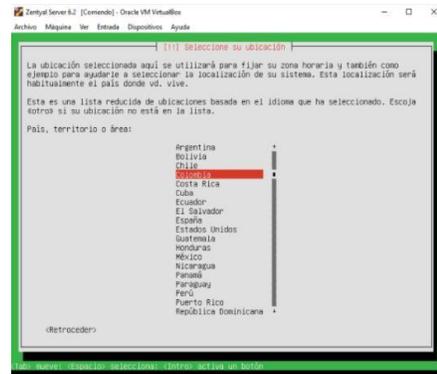


Imagen 7 - Selección país de ubicación.

Después se elige el idioma del teclado.

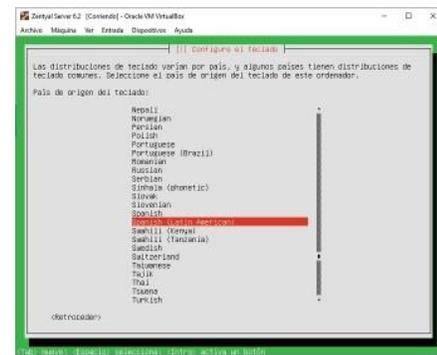


Imagen 8 - Selección idioma del teclado.

Se evidencia que comienza la instalación de Zentyal donde nombra los componentes procesados.

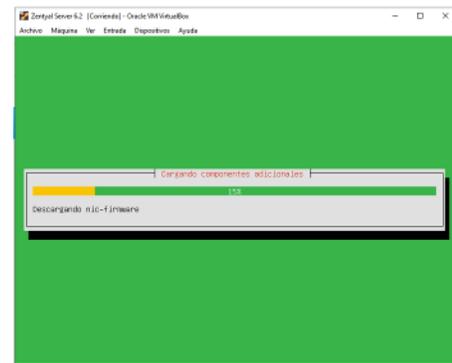


Imagen 9 - Instalación de los primeros componentes.

Después el proceso de instalación pregunta, cual es la red que debe utilizar para continuar con la descarga e instalación, en este caso se selecciona eth0 debido que es la conexión al adaptador puente que es nuestra conexión de internet.

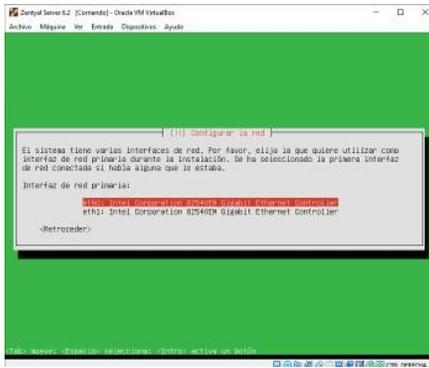


Imagen 10 - Selección adaptador de red para conexión a internet.

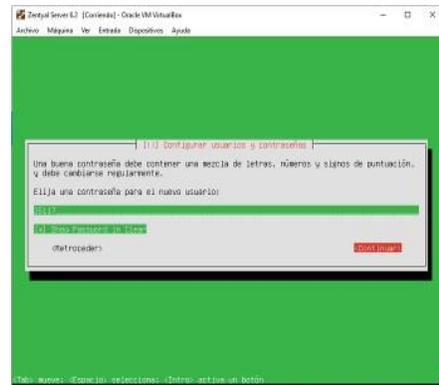


Imagen 13 - Asignar y verificar contraseña.

Seguido se asigna el nombre del servidor.

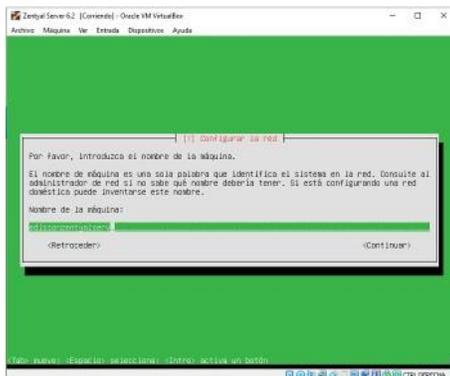


Imagen 11 - Asignación nombre "edissonzentyalserv" al servidor.

Después se visualiza la notificación de terminar la instalación donde indica validar el retiro del medio de instalación.



Imagen 14 - Finalización de la Instalación de Zentyal Server 6.2.

Se continúa asignando el nombre del usuario y contraseña, para el acceso al servidor de Zentyal.

Seguido se evidencia el escritorio de Zentyal.

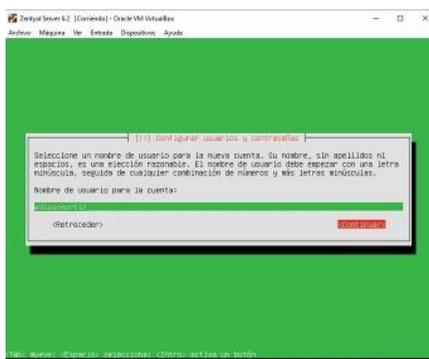


Imagen 12 - Creación usuario "edissonortiz".



Imagen 15 - Escritorio de Zentyal Server 6.2.

Se digita la contraseña del usuario y se confirma nuevamente.

Por último, se abre el inicio de sesión de la interfaz de Zentyal, es por el enlace <https://localhost:8443>, donde se accede con el usuario y contraseña que se creó en los pasos anteriores.



Imagen 16 - Inicio de sesión Zentyal.

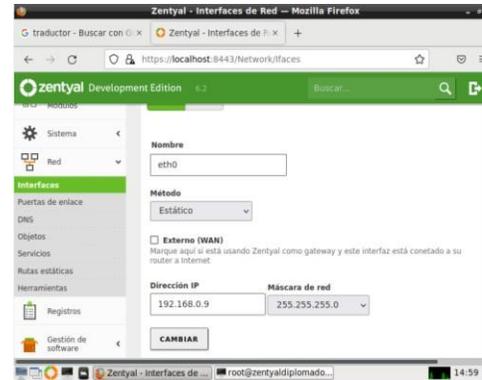


Imagen 18 - Configuración red interna.

3 TEMATICAS A DESARROLLAR

Implementar bajo Zentyal Server, los siguientes servicios de gestión de infraestructura IT:

Temática 2: Proxy no transparente.

Temática 3: Cortafuegos.

Temática 5: VPN.

3.1 TEMATICA 2: Proxy no transparente

El servicio de proxy permite ser el intermediario entre la interfaz de un usuario hacia internet, donde se procede con la configuración del proxy no transparente.

Procedemos con la instalación de los módulos Red, DHCP, DNS, NTP y Proxy para la conexión con el cliente y la funcionalidad del proxy.

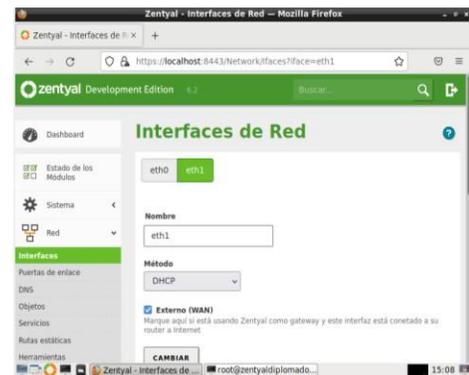


Imagen 19 - Configuración red externa.

Se procede a confirmar la puerta de enlace, en este caso es 192.168.0.1, adicional debe estar como predeterminado.

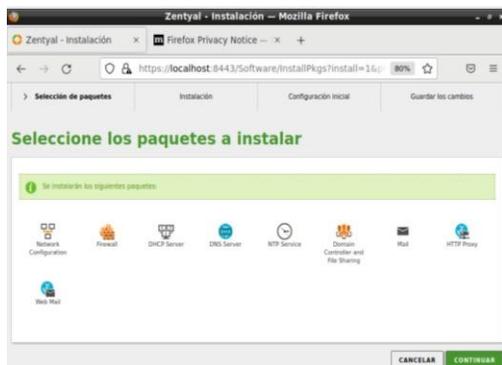


Imagen 17 - Instalación paquetes.

Seguido, se configuran dos redes, una interna estática, la cual es 192.168.0.9 y la segunda externa de método DHCP.

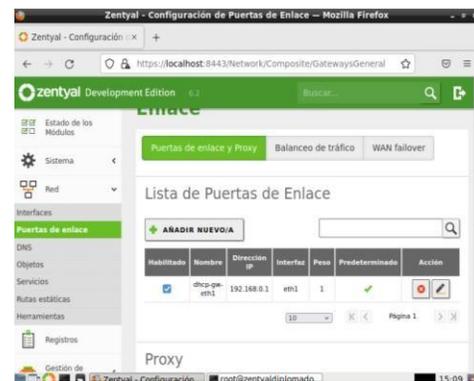


Imagen 20 - Confirmación Puerta de enlace.

Después, se crea un objeto de red, para que se asocie con la red interna de Zentyal, donde la IP de desktop1 es la IP del cliente (Desktop Ubuntu).

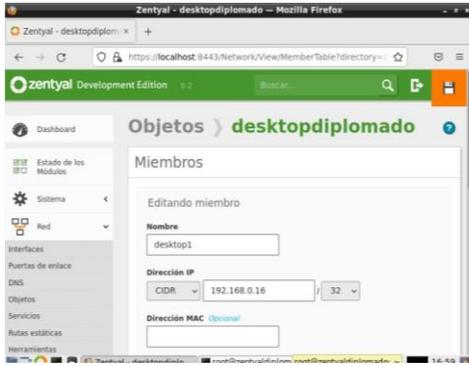


Imagen 21 - Creación de Objeto de red cliente.

Se procede a realizar la validación del puerto del proxy debido que no es transparente se mantiene el 3128.

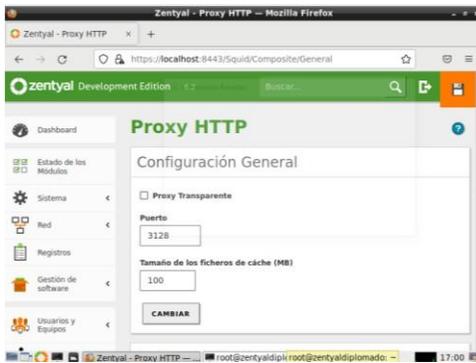


Imagen 22 - Validación puerto Proxy.

Seguido se crean unas reglas de filtrado para denegar el acceso a los DNS de ubuntu.com, unad.edu.co y youtube.com.

Donde primero se crea un perfil de filtrado en este caso Desktop, después se debe definir un umbral de filtrado, se selecciona estricto.

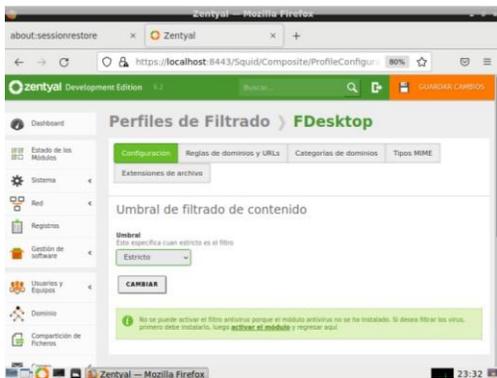


Imagen 23 - Selección del umbral del filtrado.

Se continúa agregando el dominio y la acción que debe realizar en este caso denegar.

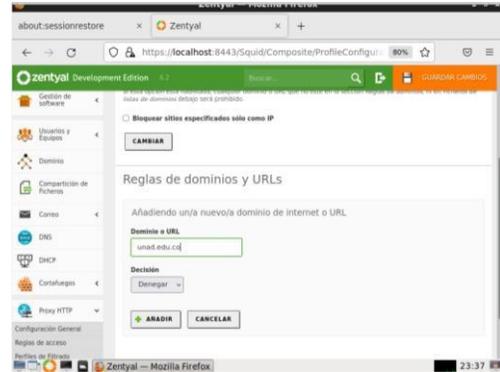


Imagen 24 - Dominios por filtrar.

Se evidencian los dominios filtrados, con las acciones de denegar.

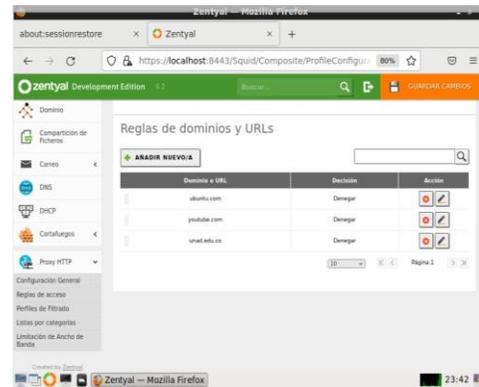


Imagen 25 - Dominios filtrados para denegar.

Después, se ingresa al cliente Desktop y se evidencia la IP asignada por DHCP.



Imagen 26 - IP asignada por DHCP en cliente.

Seguido se procede a cambiar la configuración del proxy en el navegador del cliente con la IP de Zentyal.



Imagen 27 - Cambio IP del proxy en cliente.

En la interfaz de internet, se ingresa los dominios descritos en Zentyal, Ubuntu, y Unad.edu.

Donde se evidencia el bloqueo del acceso a la pagina de Ubuntu.



Imagen 28 - Denegación ubuntu.com en cliente.

Despues se evidencia la denegación del acceso a la pagina de Unad.



Imagen 29 - Denegación unad.com en cliente.

3.2 TEMATICA 3: Cortafuegos

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. La validación del Funcionamiento del cortafuego aplicando las restricciones solicitadas, se realizará desde una estación de trabajo GNU/Linux.

Se procede a instalar los servicios de Red y Firewall.

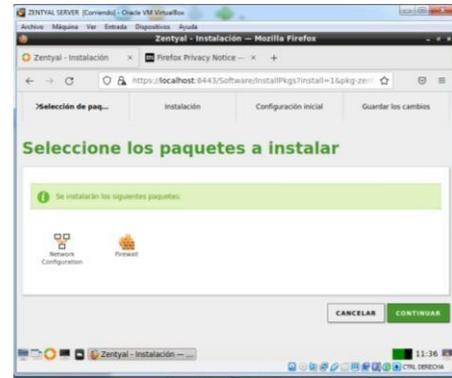


Imagen 30 - Instalación de paquetes Red y FW.

Se configura las redes para Zentyal, donde la primera es Externa de metodo DHCP.

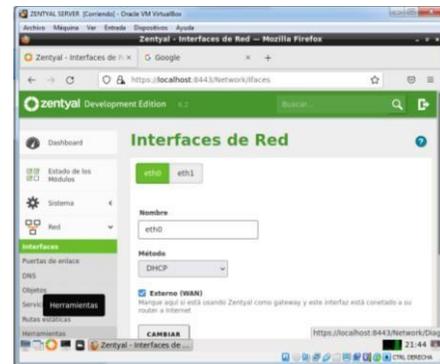


Imagen 31 - Configuración red externa servicio FW.

La segunda es Interna de metodo estatico.

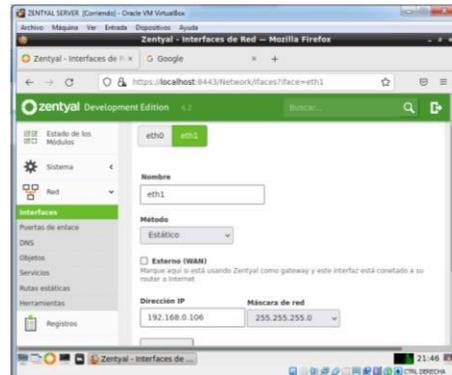


Imagen 32 - Configuración red interna servicio FW.

Se procede a configurar las reglas del firewall.



Imagen 33 - Interfaz reglas de filtrado.

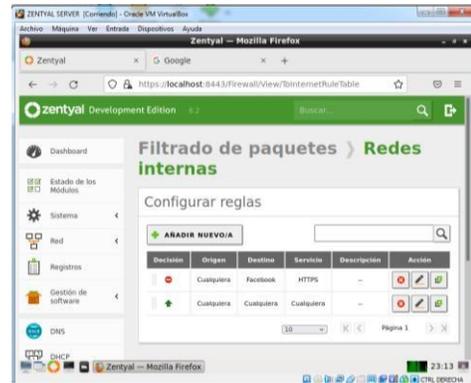


Imagen 36 - Registro de regla FW.

Empezando por la creación del objeto.

Se procede a verificar el usuario cliente, donde se evidencia que el acceso a la página de Facebook está bloqueado.

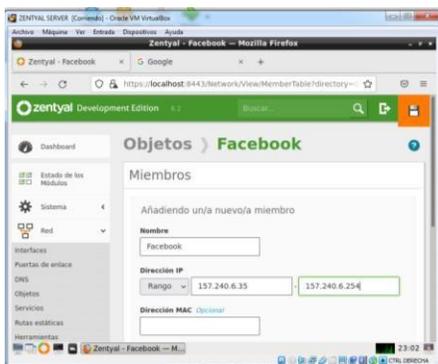


Imagen 34 - Creación de objeto Facebook.



Imagen 37 - Pagina bloqueada por Yiris Rangel.

Se procede a crear la regla del FW para generar la restricción en la red, donde se indica que la decisión es denegar el acceso.

Mientras la página de Google ingresa sin ningún problema.

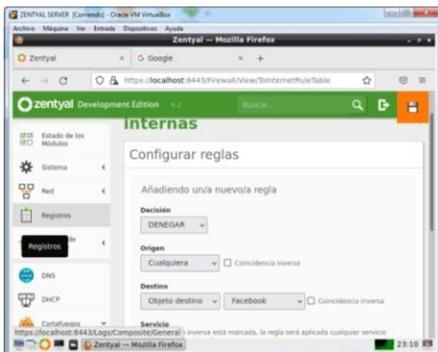


Imagen 35 - Configuración regla FW.

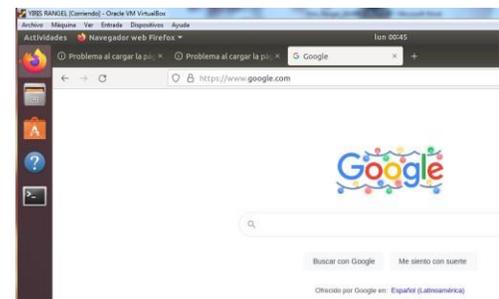


Imagen 38 - Acceso a página permitida.

Despues se evidencia la configuración de reglas, donde se evidencia la regla de denegación creada.

3.3 TEMATICA 5: VPN

VPN significa "Virtual Private Network" (Red privada virtual) y describe la oportunidad de establecer una conexión protegida al utilizar redes públicas. Las VPN cifran su tráfico en internet y disfrazan su identidad en línea, esto le dificulta a terceros el seguimiento de sus actividades en línea y el robo de datos. Una conexión VPN, permite crear una red local, sin necesidad que sus integrantes estén físicamente conectados entre sí, sino a través de Internet.

Todo el tráfico de red sigue yendo desde el dispositivo al proveedor de Internet, pero de ahí se dirige directo al servidor VPN, desde donde partirá al destino.

El Servidor abre por defecto un navegador, el cual nos muestra la interfaz gráfica principal.



Imagen 39 - Inicio de sesión Zentyal.

Luego de iniciar sesión en la Dashboard, en la parte izquierda encontramos un bloque de Módulos.



Imagen 40 - Selección de paquete VPN.

El paquete “VPN”, instala cuatro componentes.



Imagen 41 - Instalación componentes.

Se procede con la activación de los módulos de Red y VPN.



Imagen 42 - Activación módulos de Red y VPN.

Después, se selecciona el módulo de Red y se configura el adaptador 1(eth0) estático y con la Ip local que asigna Zentyal Server. El adaptador 2(eth1) estático con una nuevo rango y dirección de IP.

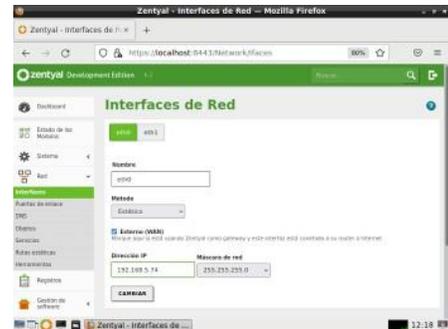


Imagen 43 - Configuración red eth0 servicio VPN.

Luego, se configura la puerta de enlace, la cual debe ser la que nos muestra el modem del servicio de internet y además le damos un nombre.



Imagen 44 - Validación puerta de enlace.

Después, en el módulo de “Autenticación de certificados”, se crea un nuevo certificado, el cual se nombró como Edison y se asigna la cantidad de días de autenticación.

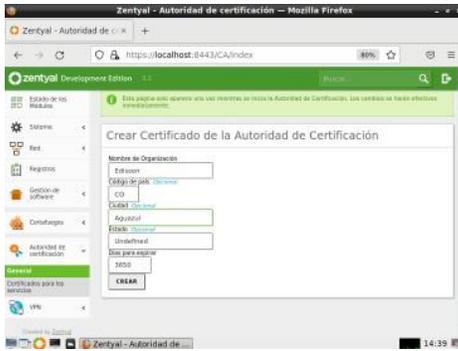


Imagen 45 - Creación del certificado.



Imagen 48 - Registro creación de servidor VPN.

Después de crear el certificado de servicios y guardado, se evidencia el certificado creado.

En el módulo de “Autenticación de certificados”, se crea un certificado para la VPN anteriormente creada (edisonort-vpn).

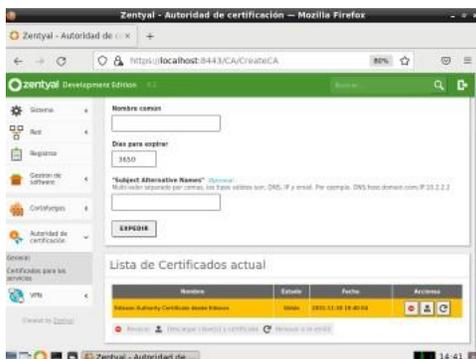


Imagen 46 - Registro de certificado creado.



Imagen 49 - Creación de nuevo certificado para el servidor.

Ahora en el módulo “VPN”, se crea un servidor, el cual se nombra como “edisonort-vpn”.

Luego de haber guardado, se evidencia el certificado creado para la VPN “edisonort-vpn”.

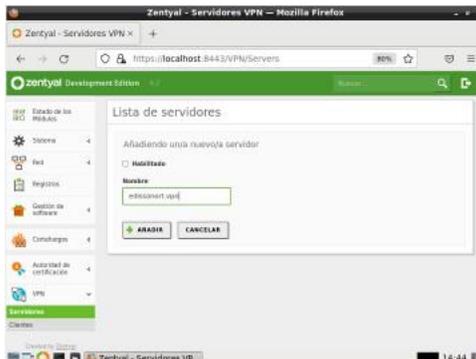


Imagen 47 - Creación de servidor VPN.

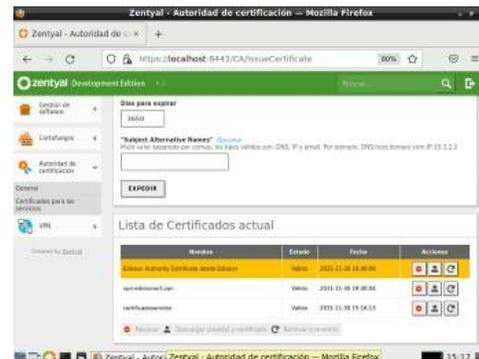


Imagen 50 - Registro de certificado creado.

Despues se evidencia el registro del servidor creado.

Después, se selecciona al icono de configuración en la VPN “edisonort-vpn”.



Imagen 51 - Configuración del servidor VPN.

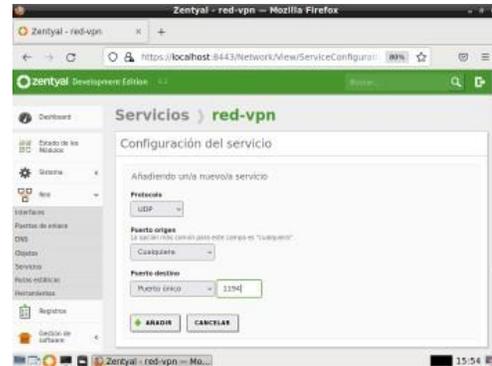


Imagen 54 - Configuración protocolo y puerto.

Seguido, se añade un nuevo servicio de red.

Luego de la configuración guardamos cambios y se visualiza el nuevo servicio.

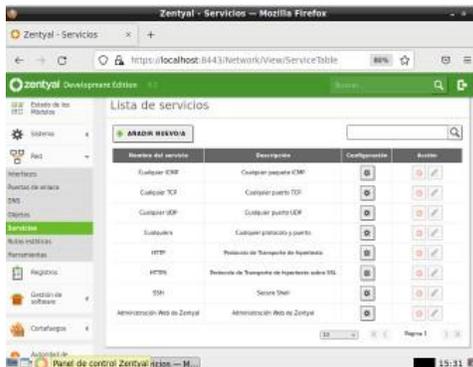


Imagen 52 - Registro de lista de servicios de red.

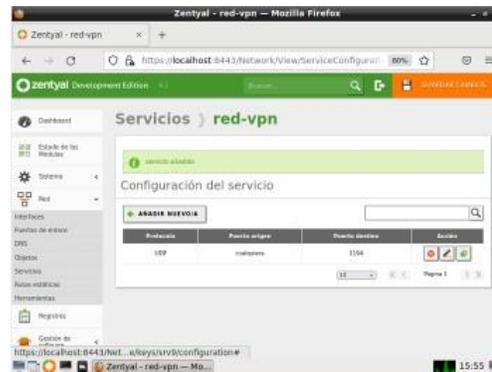


Imagen 55 - Registro del nuevo servicio.

Se asigna el servicio con el nombre “red-vpn”.

Se crea una nueva regla para la VPN.

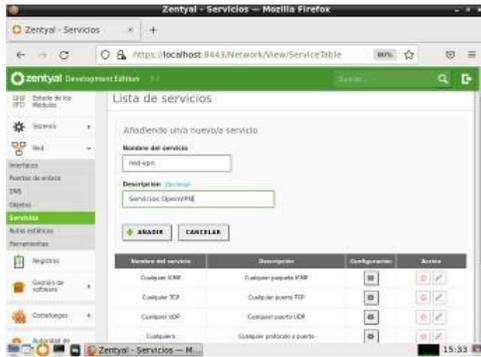


Imagen 53 - Creación nuevo servicio.

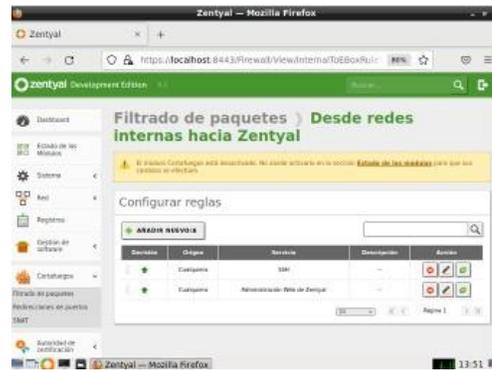


Imagen 56 - Registro de la nueva regla creada.

Seguido se ingresa al servicio y se configura con el protocolo UDP y puerto 1194.

Se crea una nueva regla, la cual va a generar permisos para todos los puertos.

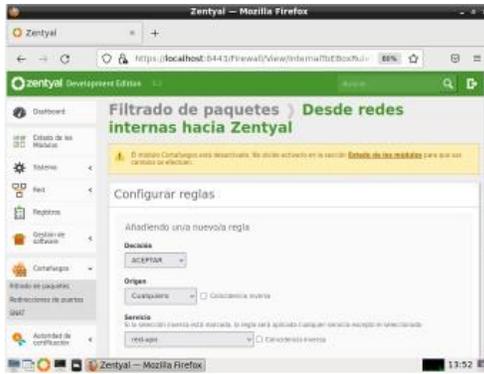


Imagen 57 - Configuración nueva regla.

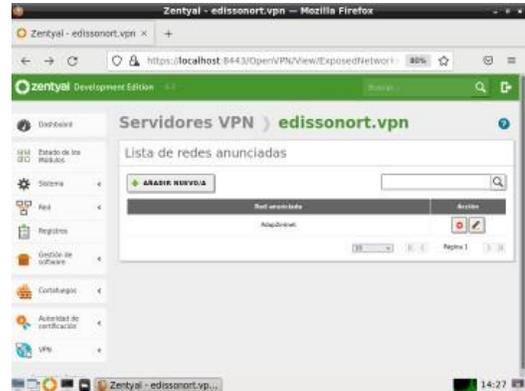


Imagen 60 - Registro de la nueva red.

Ahora se configura las redes que usará la VPN “edissonorti-vpn”.

Ahora se configura, genera y guarda los certificados de la VPN (edissonorti-vpn).

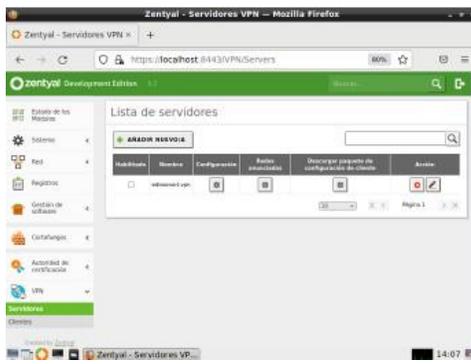


Imagen 58 - Configuración redes para el uso de la VPN.



Imagen 61 - Configuración y descarga de los certificados de servicios.

Se nombra la red “Adap2int” y se añade.

Después, se configura el certificado para el cliente (Linux), el cual, apunta al certificado generado anteriormente para la VPN y se redirecciona a la dirección Ip pública de nuestro servicio de internet.

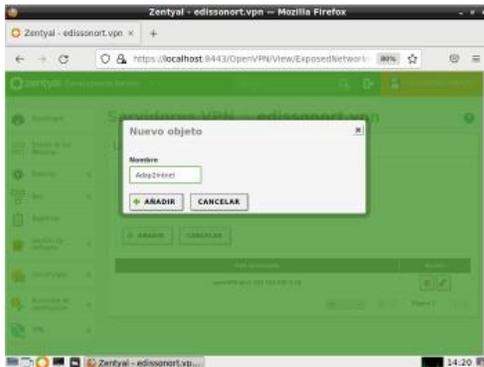


Imagen 59 - Creación nueva red Adap2int

Se evidencia la creación de la nueva red.



Imagen 62 - Configuración del servicio.

Después, se guardan los cambios y se descarga el certificado.

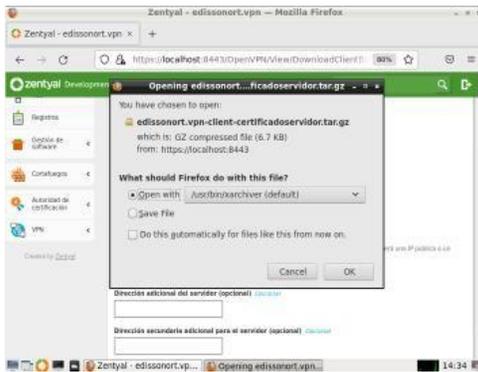


Imagen 63 - Gestión de certificado.

El archivo que se descarga es un comprimido ZIP con cuatro certificados los cuales trasladaremos a nuestro equipo cliente.

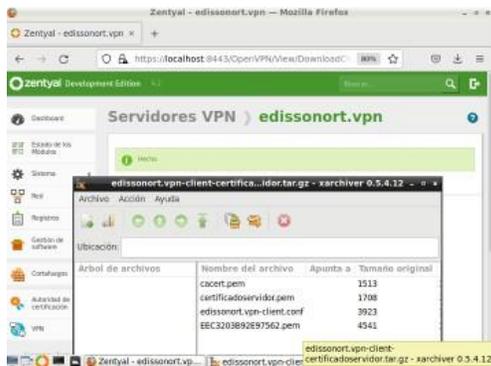


Imagen 64 - Registro de certificados.

Ya terminada toda la configuración, procedemos a habilitar la VPN “edissonort-vpn”.

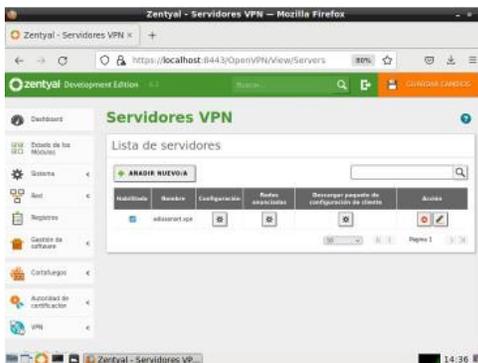


Imagen 65 - Se habilita VPN.

En la interfaz gráfica principal de la Dashboard, se evidencia que la VPN, está habilitada, la red local de Zentyal y la red de la VPN.

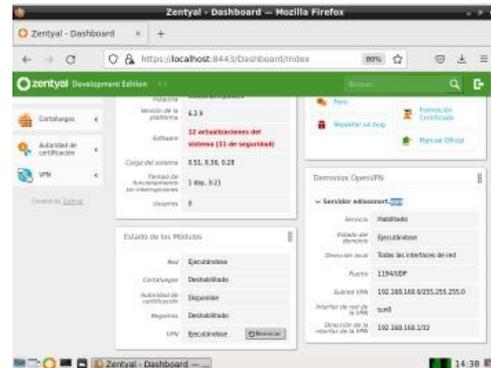


Imagen 66 - Dashboard donde se visualiza la VPN habilitada.

Ahora desde el equipo cliente Ubuntu Desktop 20.04, se instala con el comando “sudo apt-get install openvpn” la aplicación VPN.



Imagen 67 - Instalación aplicación VPN en cliente.

Luego se traslada los certificados generados en Zentyal Server al cliente y se guardan en una carpeta llamada “Certificados” en “Descargas”.



Imagen 68 - Registro de certificados.

Se procede a ingresar a la raíz de la carpeta donde están guardados los certificados.

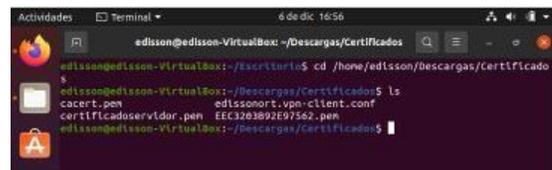


Imagen 69 - Ingreso a la carpeta donde estan los certificados.

Después se conecta el cliente con la VPN creada en Zentyal Server, se ejecuta el comando “sudo openvpn --config edissonort.vpn-client.conf”, luego de ser ejecutado se genera la conexión.

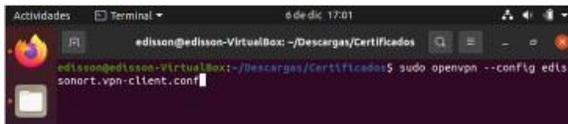


Imagen 70 - Ejecución comando para habilitar VPN.

Seguido, se evidencia la ejecución del comando anterior y como este genera el canal entre Servidor y Cliente.

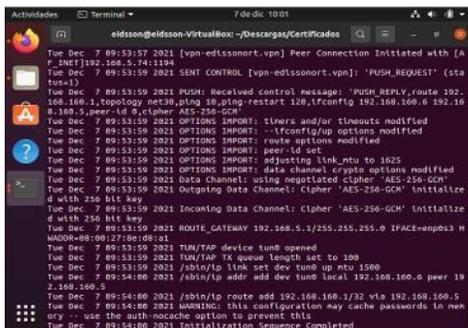


Imagen 71 - Ejecución de comando.

Luego de que finalizar la configuración de conexión, se valida con el comando “ifconfig” y se evidencia la creación de un nuevo adaptador con la dirección IP 192.168.160.6, la cual nos está apuntando a la VPN “edissonorti-vpn” creada en Zentyal Server.

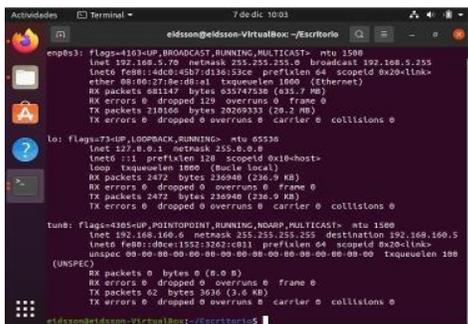


Imagen 72 - Validación de conexión a VPN.

Por último, se evidencia el adaptador con todas las descripciones de conexión con la VPN desde el cliente.

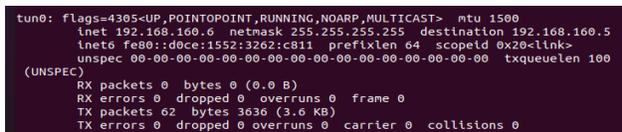


Imagen 73 - Conexión exitosa con la VPN.

4 CONCLUSIONES

En el trabajo realizado se identificaron los pasos correctos para la instalación y configuración de Zentyal Server 6.2, que es una versión estable de esta distribución y así solucionar necesidades específicas con GNU/Linux, también se realizó la configuración de la VPN en Zentyal y la instalación de la VPN creada en Ubuntu Desktop 20.04.

Se evidencia la funcionalidad y seguridad que brinda el servicio de proxy debido que permite el bloqueo de acceso a url's o dominios en específico, adicional de seleccionar el nivel de criticidad, donde se puede aplicar de forma general o a un objeto de red agregado.

La buena administración de cada uno de los servicios a través de Zentyal Server, garantiza no solo la seguridad de toda la información de las empresas, sino que además nos permite tener un mayor control sobre nuestro sistema, pues a medida que la empresa esté en crecimiento, su infraestructura seguirá creciendo, así como la cantidad de usuario que hagan uso de los diferentes servicios.

5 REFERENCIAS BIBLIOGRAFICAS

[1] Zentyal Community, Documentación de Zentyal 6.2, Servicio de Proxy HTTP. <https://doc.zentyal.org/es/proxy.html>

[2] Patrawar i, A. (2013). Getting Started with OwnCloud. (Páginas. 20 - 118). Birmingham: Packt Publishing.

<https://bibliotecavirtual.unad.edu.co/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=nlebk&AN=620016&lang=es&site=eds-live&scope=site&ebv=EK&ppid=Page- - 20>

[3] Patrawar i, A. (2013). Getting Started with OwnCloud. (Páginas. 7 - 39). Birmingham: Packt Publishing. <http://bibliotecavirtual.unad.edu.co/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=nlebk&AN=620016&lang=es&site=eds-live&scope=site&ebv=EB&ppid=pp 40>

[4] Celaya, L. A. (2014). Cloud: Herramientas para trabajar en la nube. (Páginas. 6 - 84). Recuperado de <https://elibro-net.bibliotecavirtual.unad.edu.co/es/ereader/unad/56046?page=6>