

SOLUCIONANDO NECESIDADES ESPECÍFICAS CON GNU LINUX.

Néstor Mauricio Guerrero Higuera
e-mail: nmguerrero@unadvirtual.edu.co
Jose Fortunato Palacios Hurtado
e-mail: jfpalacios@unadvirtual.edu.co
Johanna Marcela Ferro Gonzalez
e-mail: jmferrogo@unadvirtual.edu.co
Erwin Johan Collazos Estrada
e-mail: ejcollazose@unadvirtual.edu.co

RESUMEN: El artículo muestra la manera como se instala y configura Zentyal Server para utilizarse como plataforma de TI. Explica la forma de cómo se instala la plataforma y se configuran servicios de DHCP Server, DNS Server, Controlador de Dominio, proxy no transparente, cortafuegos, File Server, Print Server y VPN.

Se establecen los criterios técnicos para la implementación de la Infraestructura Tecnológica de mayor nivel para Intranet y Extranet en una institución compleja, demostrando los conocimientos adquiridos durante el desarrollo del Diplomado en Linux de la Universidad Abierta y a Distancia UNAD.

PALABRAS CLAVE: Infraestructura, Servidor, Tecnológica, Zentyal, Cortafuegos, Firewall, VPN.

1 INTRODUCCIÓN

El perfil profesional de un ingeniero de Sistemas es muy amplio, una gran parte hace referencia a la configuración de redes al interior de las empresas u organizaciones, es necesario que no solamente se realice una configuración adecuada, sino que se tenga muy en cuenta la seguridad de estas redes especialmente por la cantidad de información.

Este trabajo presenta paso a paso la instalación, configuración y puesta en funcionamiento de Zentyal Server para configurar redes al interior de una organización y conectarlas a través de infraestructuras tecnológicas con internet, utilizando los protocolos de seguridad adecuados para estos casos.

También se presenta la configuración del servidor Proxy el cual es una red informática que hace de intermediario en las peticiones de recursos que realiza un cliente a otro servidor, sin contar que se realiza la configuración de cortafuego el cual nos permitirá bloquear el ingreso a personas no autorizadas y así poder crear la VPN que nos ayuda a conectar computadoras a la red privada.

2 INSTALACIÓN DE ZENTYAL SERVER COMO SISTEMA OPERATIVO

2.1 CONFIGURACIÓN DE LA MÁQUINA VIRTUAL

Para la instalación de Zentyal como sistema operativo se creó una máquina basada en Linux Ubuntu con una memoria RAM de 2 GB, un disco duro de 20 Gb, dos adaptadores de red uno para la conexión LAN y otro para la conexión WAN. Se descargó la imagen .iso de <http://download.zentyal.com/zentyal-6.2-development-amd64.iso> (Documentación de Zentyal, 2021).

2.2 PROCESO DE INSTALACIÓN

Luego de montar la imagen .iso en la máquina virtual se arranca e inicia el proceso de instalación, seleccionando el idioma, posteriormente seleccionando la instalación a realizar (Murillo, 2020).

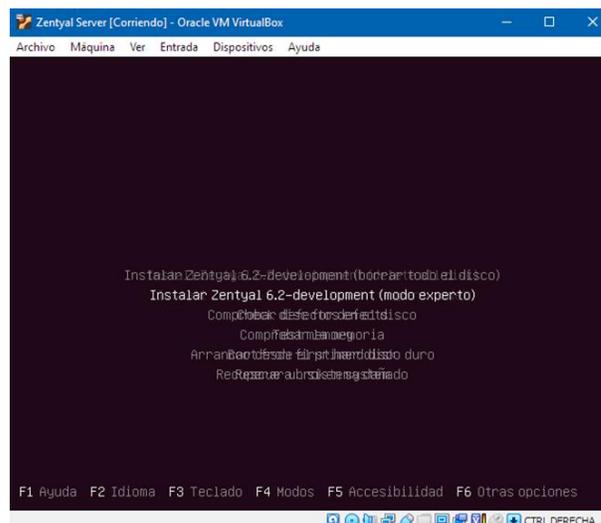


Figura 1. Selección modo de instalación Zentyal.

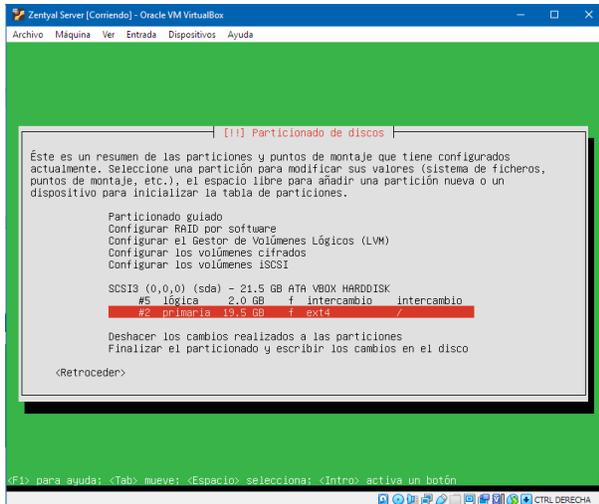


Figura 2. Configuración de disco duro

Para esta ocasión se seleccionó el modo experto, posteriormente se selecciona la ubicación, la distribución de teclado, posteriormente la pantalla nos muestra los adaptadores de red que tiene la máquina, se selecciona el usuario y contraseña para la máquina en que se instalará Zentyal, y se procede a configurar las particiones del disco duro.

Continuando (sda) con la selección de la instalación del entorno gráfico, para mejorar la respuesta de la máquina virtual se decidió no instalar este entorno gráfico, luego se configura el proxy, en caso de ser necesario y la instalación del cargador de arranque.

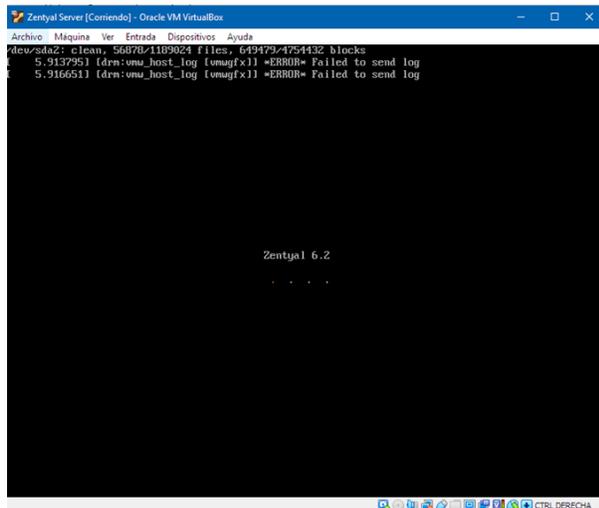


Figura 3. Arranque de Zentyal

Posterior a la instalación se procede a iniciar sesión con el usuario y contraseña configurados durante la instalación, luego ingresar se hace la actualización y para acceder de manera gráfica se hace desde una máquina externa a través del navegador web.

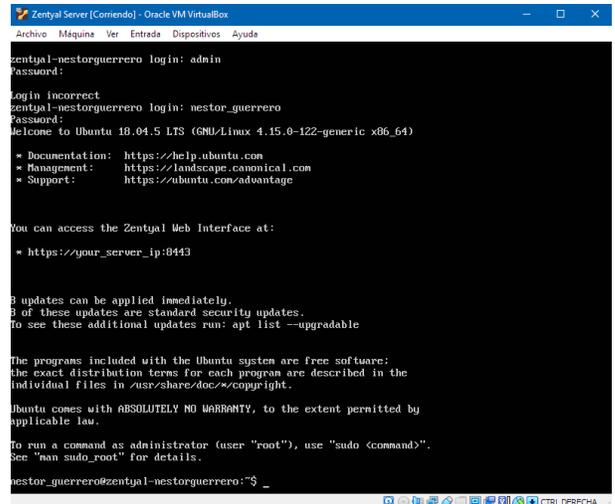


Figura 4. Iniciando sesión en Zentyal

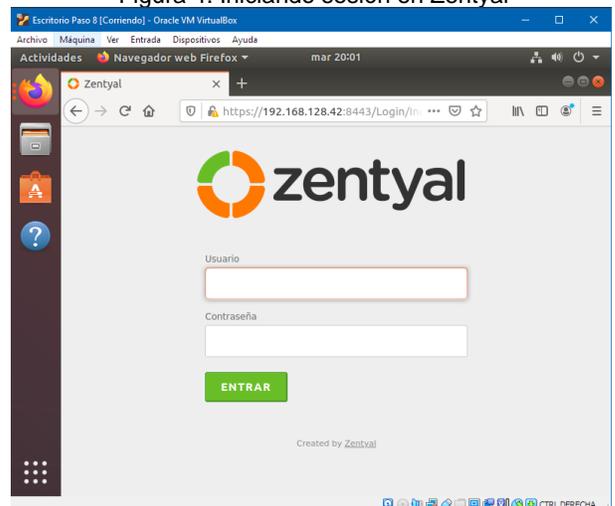


Figura 5. Arranque de Zentyal

A partir de esta conexión se continua con la configuración de los diferentes módulos de Zentyal..

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

Una vez instalado Zentyal, se procede a realizar su configuración inicial, instalando los módulos DHCP Server, DNS Server y Controlador de Dominio.

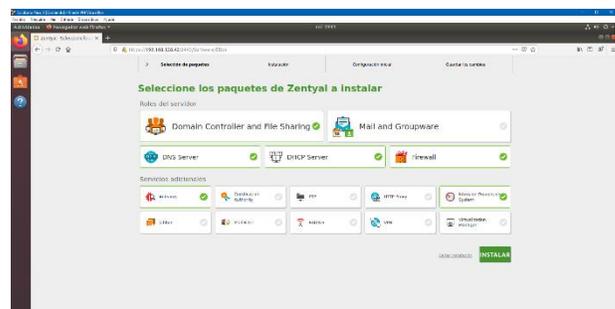


Figura 6. Página de selección de módulos a instalar

Luego de un tiempo en el que se instalan los módulos, se configuran las interfaces de red para las conexiones WAN y LAN.

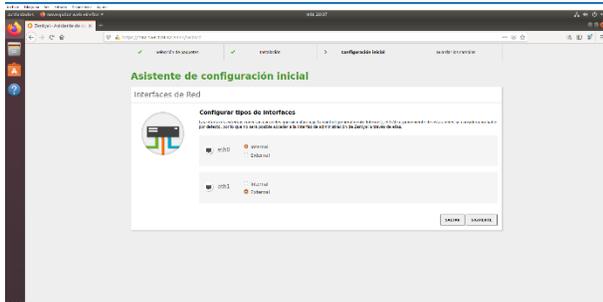


Figura 7. Página de configuración de interfaces de red

Finaliza la configuración inicial después de un tiempo, se abre la página del entorno gráfico de Zentyal en el Dashboard, en donde se pueden observar las actualizaciones necesarias que se requieren para continuar con la configuración de los módulos.

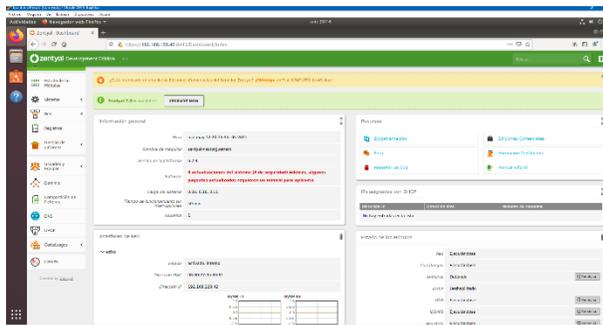


Figura 8. Dashboard Zentyal

Una vez realizadas las actualizaciones se procede a verificar la instalación de los módulos a utilizar:

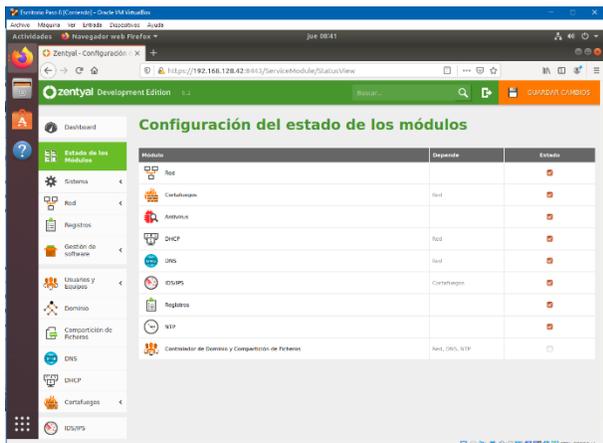


Figura 9. Estado de los módulos en Zentyal.

3.1 CONFIGURACIÓN DE DHCP SERVER

Una vez que se ve el módulo de DHCP se ingresa a su configuración, por ahora definiendo la red LAN, la dirección de Zentyal.

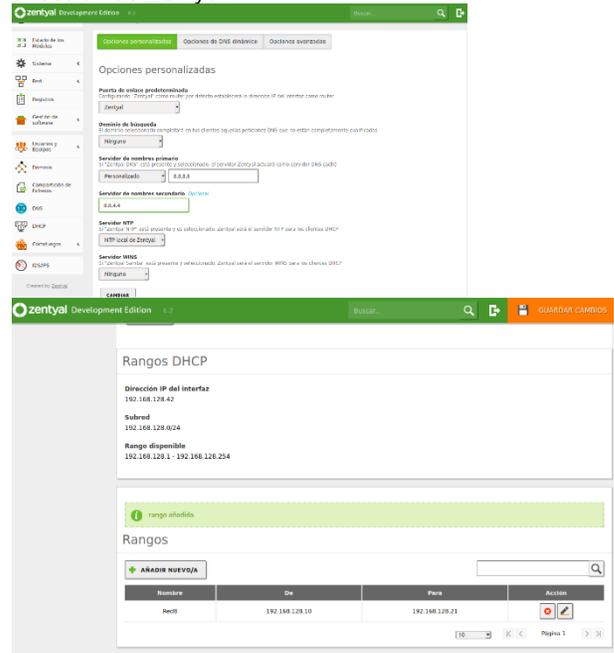


Figura 10. Configuración de DHCP server

Para comprobar la conexión de los equipos a través de la red interna se hace desde Zentyal a Ubuntu mediante el comando ping.

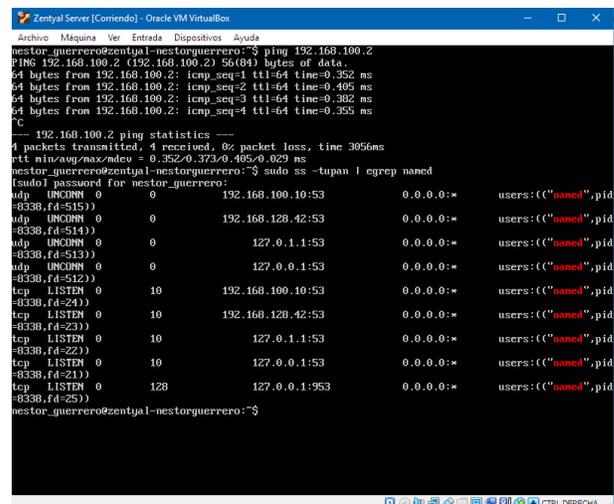


Figura 11. Comprobando la conexión de la red.

3.2 CONFIGURACIÓN DE DNS SERVER

Una vez revisado que está instalado el módulo DNS en Zentyal se procede a configurar y a poner en funcionamiento.

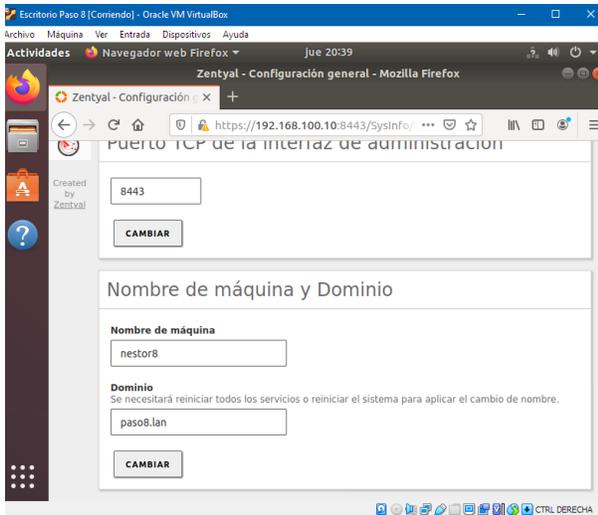


Figura 12. Configuración de nombre de máquina y dominio.

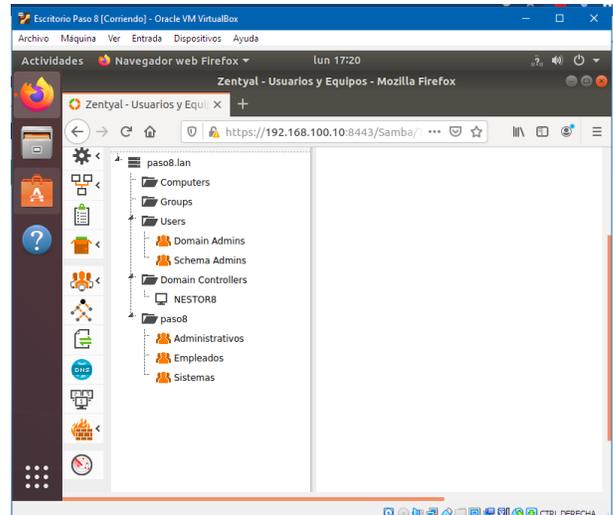


Figura 14. Creación de unidades administrativas y grupos.

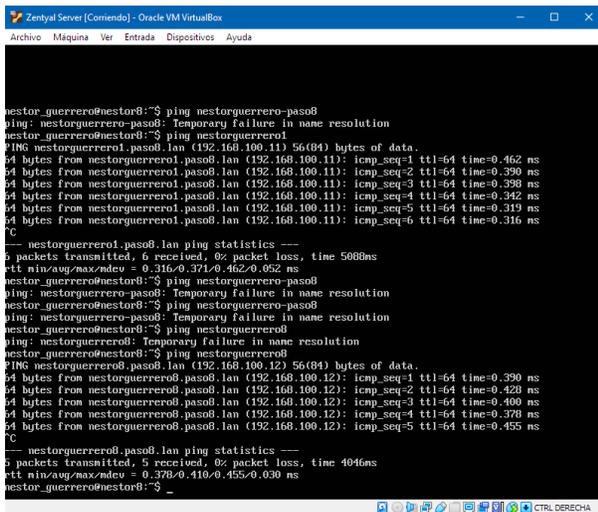


Figura 13. Comprobación del funcionamiento de DNS server.

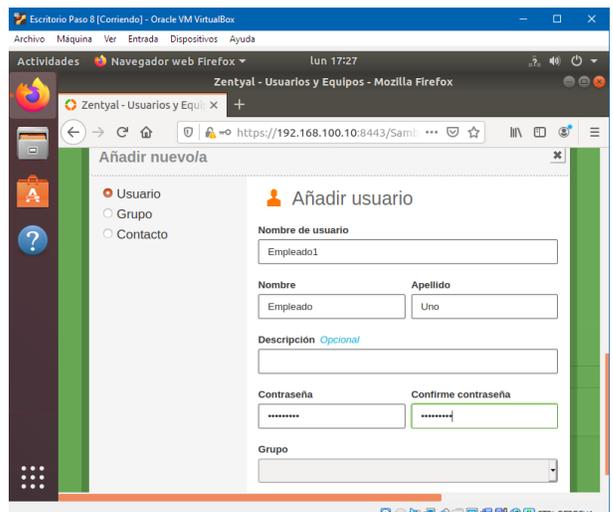


Figura 15. Creación de usuarios.

3.3 CONFIGURACIÓN DE CONTROLADOR DE DOMINIO

Luego de instalar el módulo controlador de dominio se procede a crear las unidades administrativas, grupos de usuarios y usuarios para el acceso a las redes.

4 TEMÁTICA 2: PROXY NO TRANSPARENTE ESPERADO PRODUCTO

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.

4.1 SE SELECCIONAN LOS PAQUETES NECESARIOS

En este paso luego de instalar zentyal seleccionamos los paquetes a utilizar con Proxy



Figura 21. Tipo de servidor

4.7 INSTALACIÓN CON ÉXITO

Aquí podemos observar que la instalación fue exitosa

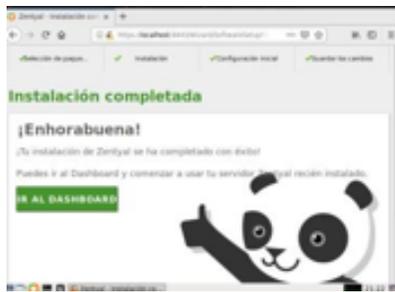


Figura 22. Instalación terminada

4.8 ZONA DE DHCP

Entramos a la zona de DHCP, en las interfaces se da clic al botón de configuración

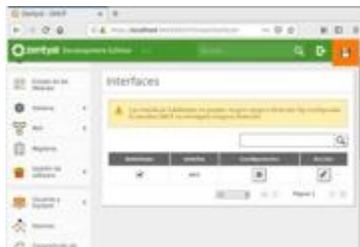


Figura 23. Zona DHCP

4.9 SECCIÓN DE RED

En la sección de red, en las interfaces se configura la red eth0 en DHCP para la comunicación con la red WAN.



Figura 24. Interface de red

4.10 SE CONFIGURA LA RED

Se configura la red eth1 en estático y se asigna una ip.



Figura 25. Configurar red

4.11 OBJETO EN LA RED

En esta fase se crea un objeto en la parte de red

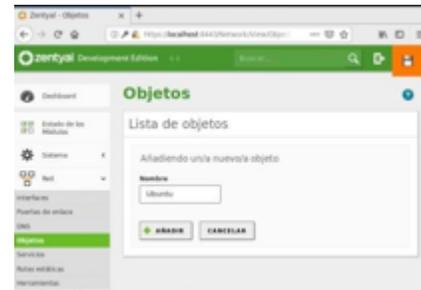


Figura 26. Se crea objeto

4.12 NUEVO MIEMBRO PARA EL OBJETO

Se crea un nuevo miembro para el objeto de red



Figura 27. Nuevo Miembro

4.13 CONFIGURACIÓN DEL PROXY TRANSPARENTE

Se configura el proxy transparente y el puerto por el cual va a escuchar



Figura 28. Configuración de Proxy

4.14 CONFIGURACIÓN DE LA REGLA DE ACCESO

Se configura la regla de acceso para el objeto previamente creado, donde se deniega todas las peticiones



Figura 29. Regla de acceso

4.15 PRUEBA QUE EL PROXY ESTÉ FUNCIONANDO

Se visualiza la prueba que el proxy está funcionando y está bloqueando la navegación en el equipo

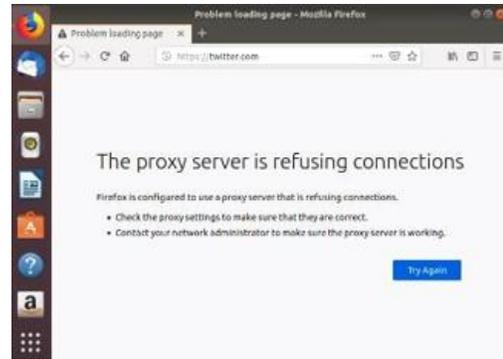


Figura 30. Prueba de Proxy

5 TEMÁTICA 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 hará desde una estación de trabajo GNU/Linux (Perez, 2019).

5.1 SELECCIONAMOS EL MODULO DEL CORTAFUEGOS (FIREWALL) PARA CONFIGURARLO

Revisamos en el menú **Gestión de Software**, luego damos clic en **componentes de Zentyal**. Aquí seleccionamos Firewall y le damos clic en Instalar para montar este paquete.

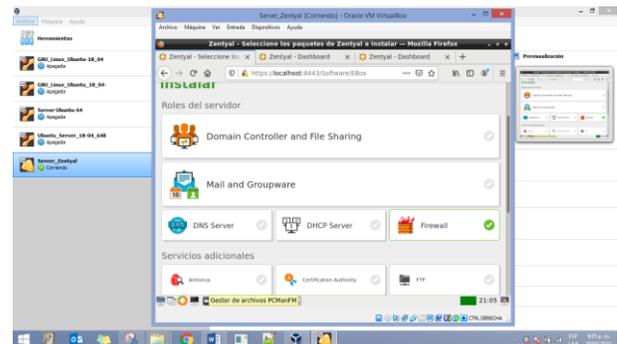


Figura 31. Selección de Modulo Cortafuegos (firewall)

Revisamos en la siguiente ventana nos informará que se instalarán 2 paquetes, el del Firewall y el de Red, esto debido a que para configurar el Cortafuegos necesitamos el módulo de la Red. Damos clic en el boto Continuar para confirmar que si queremos que se instalen dichos componentes al Zentyal.

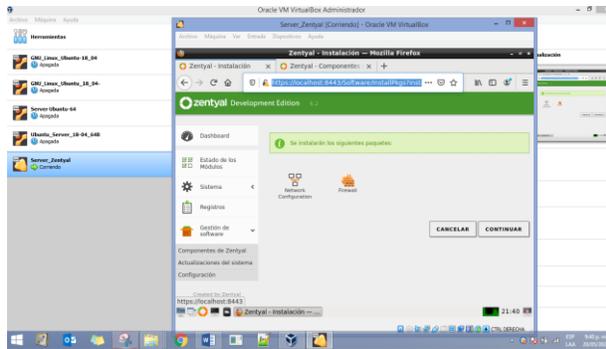


Figura 32. Paquetes a instalar

Damos clic en el botón OK para finalizar la instalación.

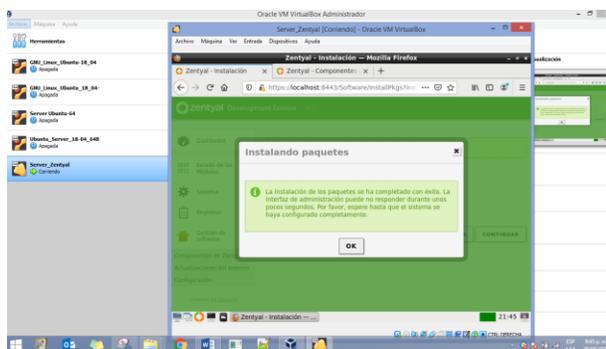


Figura 33. Confinación de instalación de Módulo

5.2 ACTIVACION DE MODULOS INSTALADOS

Validamos en el menú de **Estado de los Módulos** y activamos el Cortafuegos incluyendo el de Red para poderlos usar y configurar.

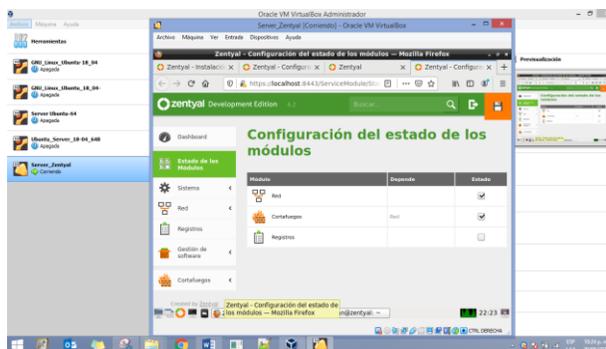


Figura 34. Activación de módulos

5.3 CONFIGURACION DE INTERFACES DE RED EN ZENTYAL

Primero nos aseguramos que el dispositivo tenga configurado mínimo un Adaptador de Red Interna y un Adaptador Puente desde Virtual Box.

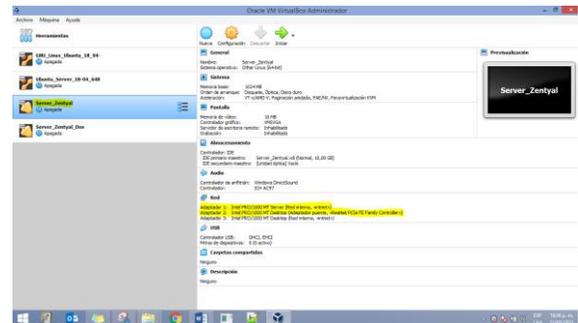


Figura 35. Revisión y configuración de Adaptadores

Ahora en el servidor Zentyal Vamos al menú de Red y damos clic en Interfaces. Aquí vamos a configurar 2 redes que necesitamos. Una primera que debería contener la IP del Router (Interfaz de red **eth0**) la cual deber ser marcada como externa.

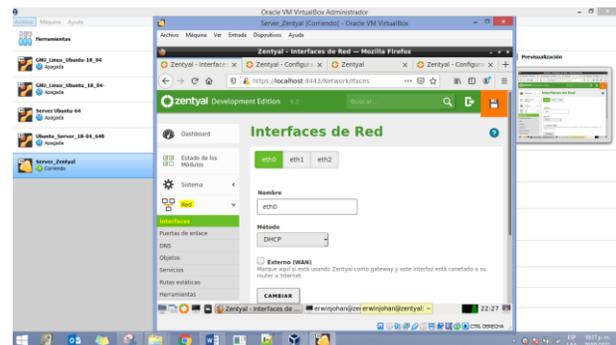


Figura 36. Configuración Interfaz de Red eth0

Ahora vamos a configurar la segunda red (Interfaz de red **eth1**). Esta la configuramos como estática y procedemos a asignar la IP (**192.168.0.10**) a nuestro Adaptador puente, con esto creamos la red Interna hacia Ubuntu Desktop.- Al finalizar guardamos los cambios.

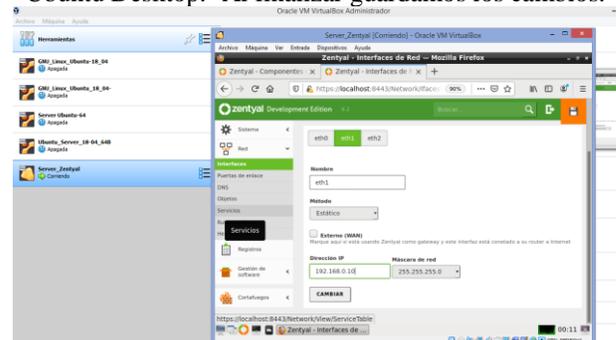


Figura 37. Configuración Interfaz de Red eth1

5.4 VERIFICACION DE RED EN UBUNTU DESKTOP

Primero revisamos en el Dispositivo que el tipo de Adaptador en Virtual Box sea de Red Interna.

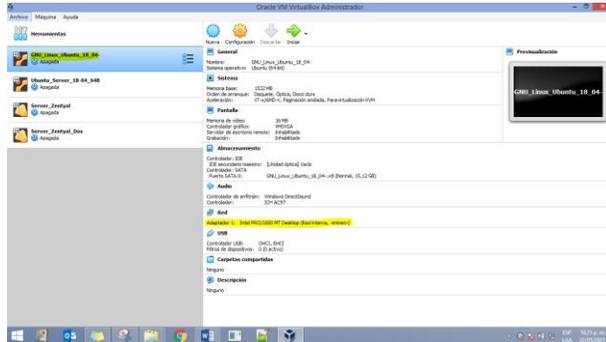


Figura 38. Verificación tipo de adaptador en Ubuntu

En el Ubuntu Desktop vamos a la opción de red y le damos en configurar para asignar la IP de nuestra Red Interna

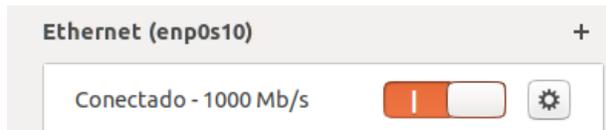


Figura 39. Selección

Apreciamos que Inicialmente aparecen los datos de las IP que se asigna el Adaptador de Red dependiendo del Router.

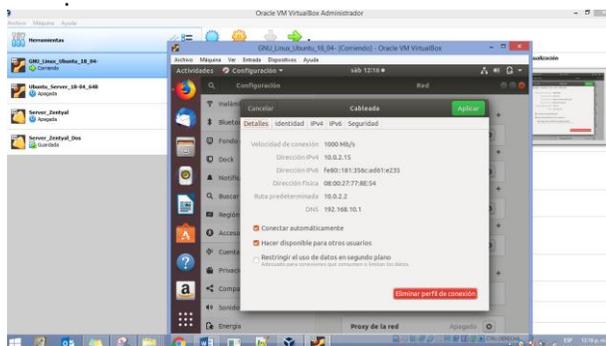


Figura 40. Verificación de IP en adaptador

5.5 CONFIGURACION DE RED EN UBUNTU DESKTOP

Configuramos manualmente, para esto vamos a **IPv4**, aquí le asignamos a este escritorio la IP (**192.168.0.15**) para que quede dentro del mismo dominio de red, le damos la misma mascara de red que tiene nuestro Router (255.255.255.0) y por ultimo le agregamos nuestra Puerta de Enlace, que en este caso es la IP de nuestro Adaptador en el servidor Zentyal (192.168.0.10). Para guardar le damos en el botón Aplicar.

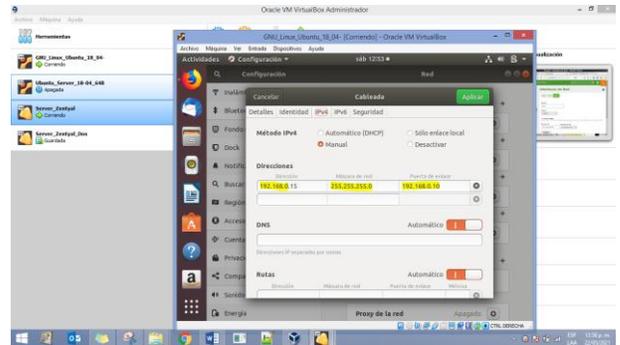


Figura 41. Configuración de Red en Ubuntu Desktop

Revisamos que hayan quedado aplicados los cambios ingresados.

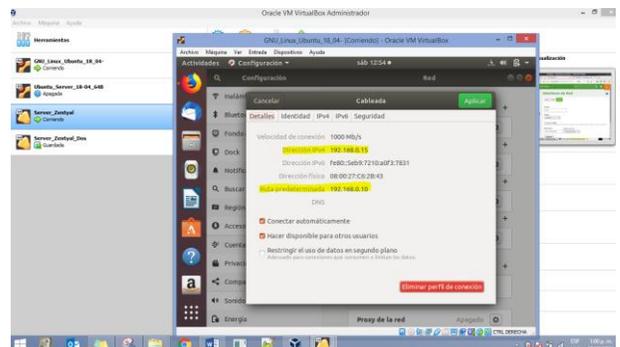


Figura 42. Revisión de Red después del cambio

5.6 REGLAS DE FILTRADO EN EL CORTAFUEGOS DE ZENTYAL

Damos clic en la sección de **Cortafuegos** (firewall) del menú a la izquierda en servidor ZENTYAL.

Buscamos la opción de **Reglas de filtrado para las redes internas** y damos clic en el botón **Configurar Reglas**

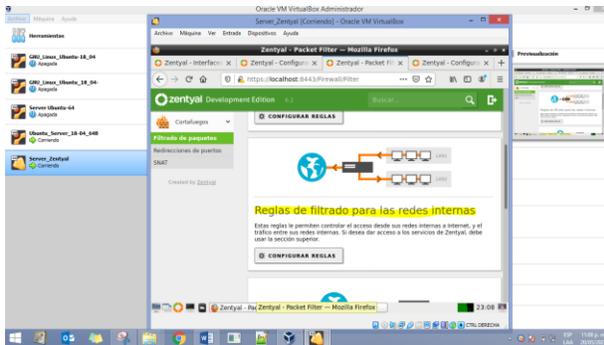


Figura 43. Reglas de Filtrado para redes internas

5.7 CREACION DE REGLA EN EL CORTAFUEGOS DE ZENTYAL PARA PERMITIR ACCESO A CUALQUIER PAGINA WEB

Damos clic en **Añadir Nuevo/a** para crear una regla de filtrado. En el formulario diligenciamos los datos solicitados y por ultimo le damos en el botón **Añadir**. En este caso **Añadimos** una regla para permitir acceso a cualquier página web sin restricción.

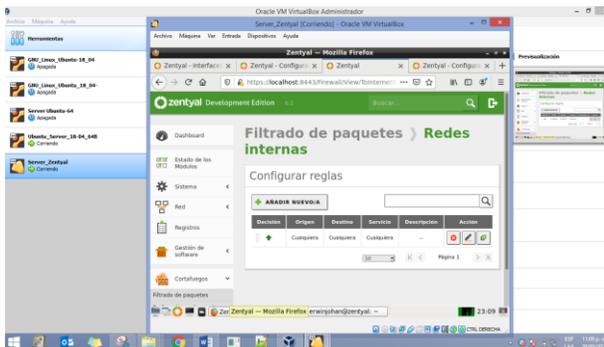


Figura 44. Reglas de Filtrado

En este caso **Añadimos** una regla para permitir acceso a cualquier página web sin restricción.

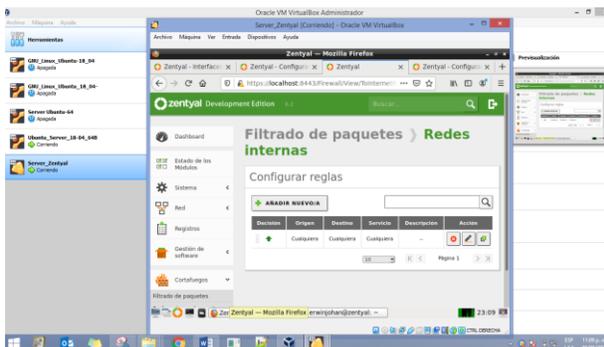


Figura 45. Regla de Filtrado para permitir accesos

5.8 VERIFICACION ACCESO A REDES SOCIALES EN UBUNTU DESKTOP

Revisamos en nuestro Ubuntu Desktop que se pueda abrir un portal de red social. En este caso (**Facebook**) y confirmamos que si está funcionando la url (<https://www.facebook.com>)

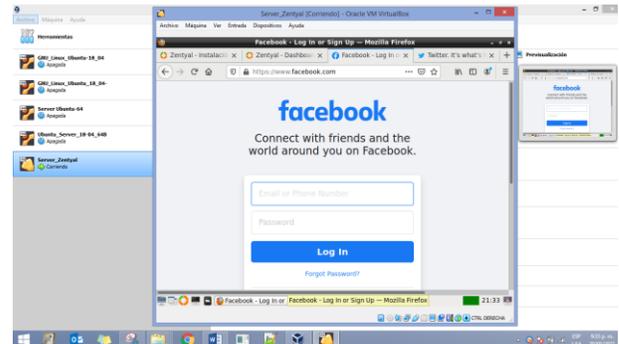


Figura 46. Consulta de portal Facebook

Ahora también Consultamos en **Twitter**

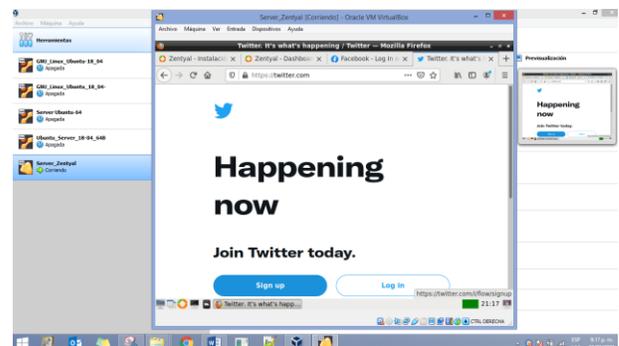


Figura 47. Consulta de portal de Twitter

5.9 CONSULTAMOS IP DE RED SOCIAL

Ingresamos a la consola y hacemos ping a la página que queremos denegar la IP, en este caso (www.facebook.com), entonces digitamos el comando **ping www.facebook.com** y damos Enter. De esta manera podemos ver que IP está contestando y así denegándola.

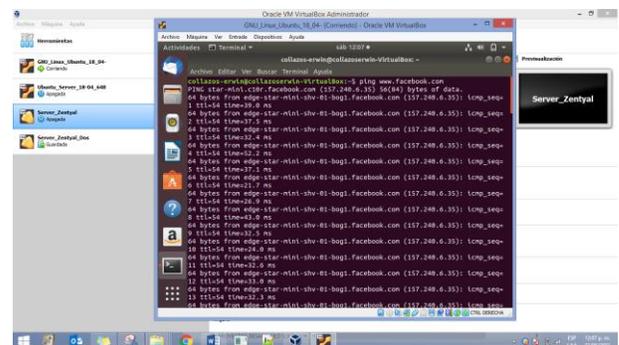


Figura 48. Consultar Ip de red social en consola

5.10 CREACION DE REGLA EN EL CORTAFUEGOS DE ZENTYAL PARA DENEGAR ACCESO A RED SOCIAL

Teniendo el dato de la IP está contestando, En el menú de Cortafuegos, vamos a Filtrado de Paquetes y damos clic en **Añadir Nuevo/a** para crear una regla de filtrado para Denegar el acceso a una Red social, en este caso a Facebook. (IP 157.240.6.35) según nos arrojó la consulta.

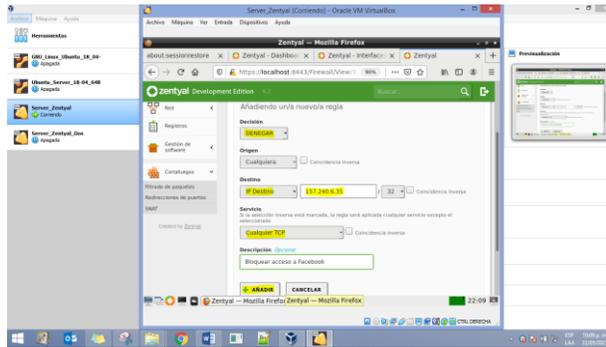


Figura 49. Formulario para Denegar acceso

Nos quedaría así la configuración, Una regla para dar acceso a cualquier portal y una que bloquee el acceso a Facebook

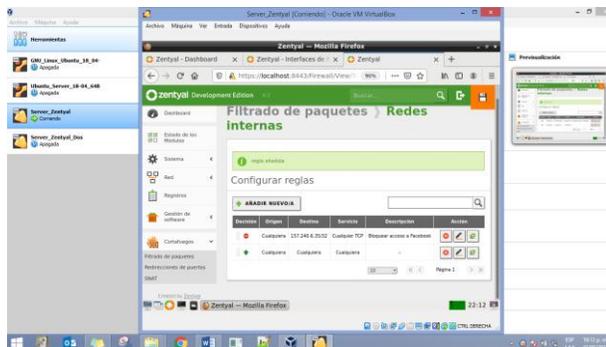


Figura 50. Reglas de filtrado añadidas

5.11 VALIDACION DE NEGACION DE ACCESO A RED SOCIAL EN UBUNTU DESKTOP

Revisamos nuevamente en nuestro escritorio de Ubuntu si podemos acceder al portal de Facebook.

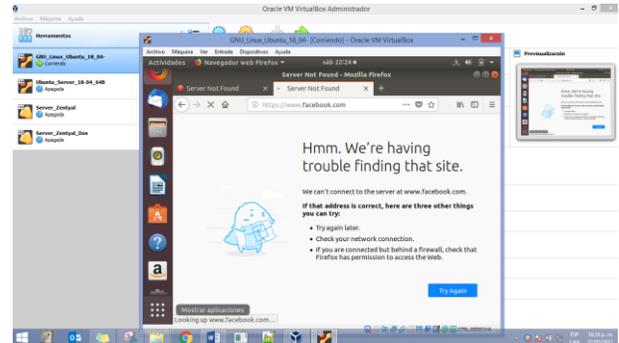


Figura 51. Revisión de acceso a Facebook

Cuando queramos permitir el acceso nuevamente vamos al servidor **Zentyal** y en **Cortafuegos** eliminamos la regla de Denegar este acceso y ya queda restablecido el acceso.

6 TEMÁTICA 5: VPN

Una vez instalado Zentyal, se procede a realizar su configuración inicial, instalando el módulo VPN. Donde adicionalmente en la selección de paquetes a instalar se instalarán los paquetes de Certification Authority, Firewall, Network Configuración y VPN (Zentyal Community, 2015).

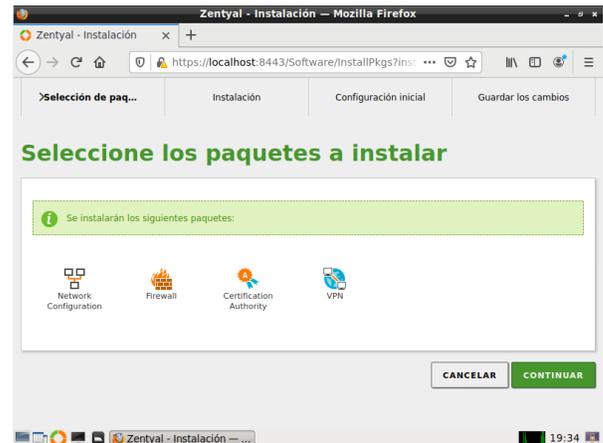


Figura 52. Paquetes a instalar.

6.1 CERTIFICACIÓN Y CONFIGURACIÓN DE SERVIDOR VPN

Una vez realizada la configuración inicial contenida por la configuración de las interfaces, el sistema empieza a guardar dicha configuración. Una vez hecho esto, se cargará la Dashboard, en la cual en la parte izquierda mostrará las distintas opciones que tiene disponible, allí, se deberá ir inicialmente a Autoridad de Certificación/General, esto, para expedir un certificado que permita la implementación del servidor VPN.

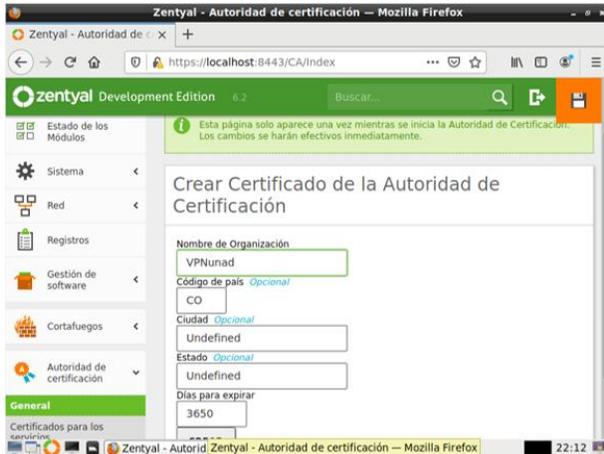


Figura 53. Certificado para servidor vpn.

Una vez creado el certificado para el servidor VPN se puede continuar a añadir un nuevo servidor VPN, esto, desde VPN/Servidores, que estará ya habilitado.

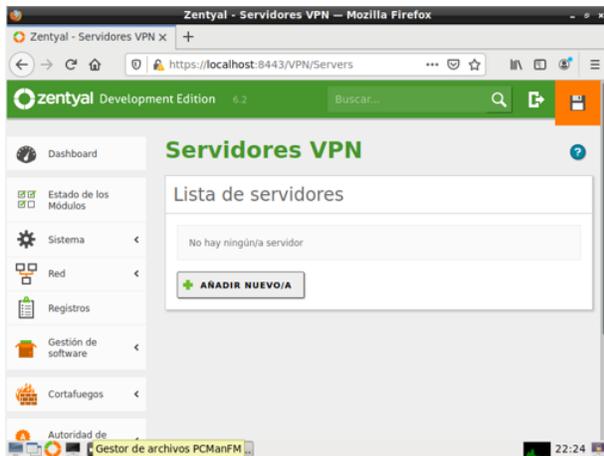


Figura 54. Función de servidor vpn habilitada

Después de añadir un nuevo servidor, se le asignará un nombre y se añadirá, una vez hecho esto, mostrará lo siguiente:

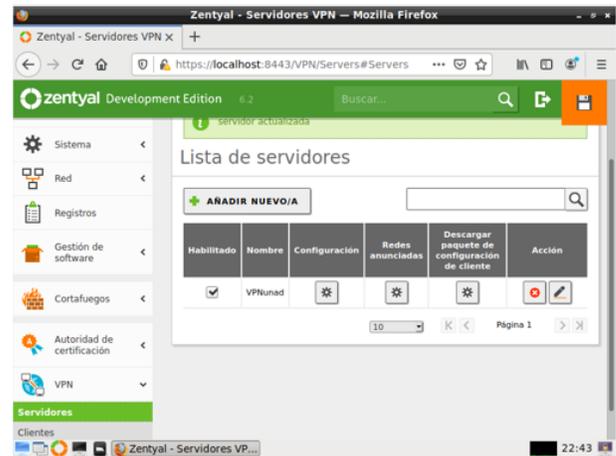


Figura 55. Servidor vpn añadido.

Siiguiente a el añadimiento del nuevo servidor VPN, se procede a configurarle los parámetros en los que funcionará. En esta configuración se le asignará un puerto, una dirección VPN, el certificado anteriormente creado para el servidor VPN y los parámetros necesitados.

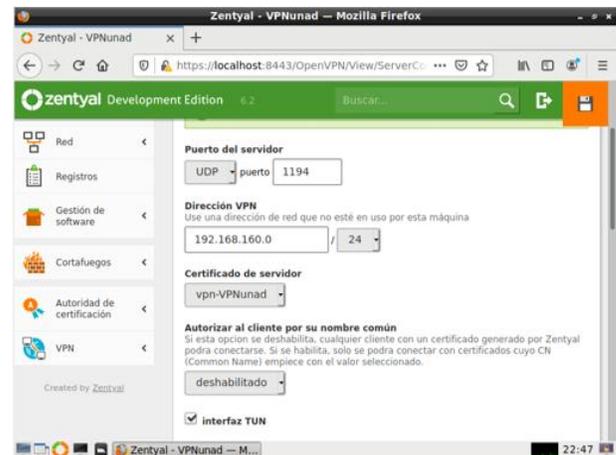


Figura 56. Parámetros de configuración en servidor vpn.

6.2 CERTIFICACIÓN Y CONFIGURACIÓN DE USUARIO

Para que un usuario pueda hacer uso del servidor VPN se deberá crear un certificado que le permita al usuario hacer uso de este servidor. Para ello, nuevamente en Autoridad de Certificación/General se expide un certificado para el usuario.

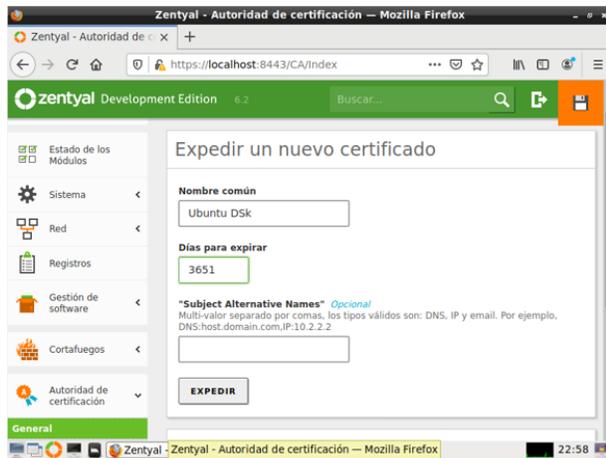


Figura 57. Certificado para usuario.

Una vez expedido el certificado para el usuario, nuevamente en Servidores VPN se escoge la opción de “Descargar paquete de configuración de cliente”, después cargará la ventana donde se deberán configurar los parámetros del usuario donde se seleccionará el tipo de usuario, el certificado del usuario, tipo de conexión y dirección del servidor, la cual deberá ser una IP estática.

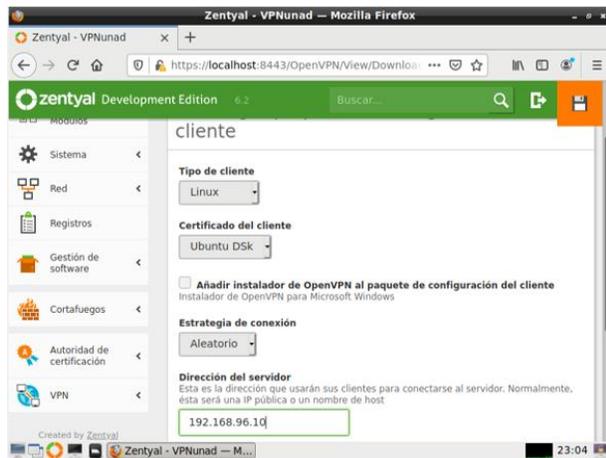


Figura 58. Parámetros de configuración del cliente.

Este generará un paquete de configuración para el cliente y que así se pueda configurar los parámetros de configuración en el equipo del cliente de manera más sencilla.

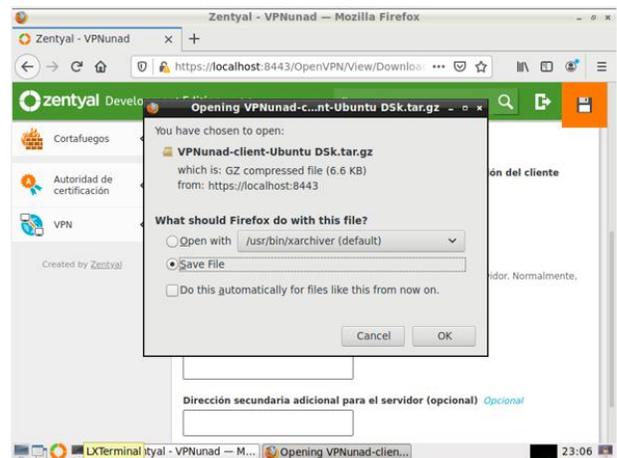


Figura 59. Paquete de configuración para cliente.

Ahora desde el cliente se añade una nueva VPN, esto, desde configuración de red del equipo, donde si no es posible mover el paquete de configuración previamente descargado en el servidor, se escogerá un el “Protocolo de túnel punto a punto (PPTP)”.



Figura 60. Añadiendo vpn en cliente.

Una vez seleccionado el protocolo, se define un nombre con el que se identificará en el equipo (este nombre no afecta la configuración y funcionamiento), y se le agrega la pasarela, que es la IP configurada en los parámetros del cliente en el servidor. Después de esto se seleccionará la configuración avanzada.

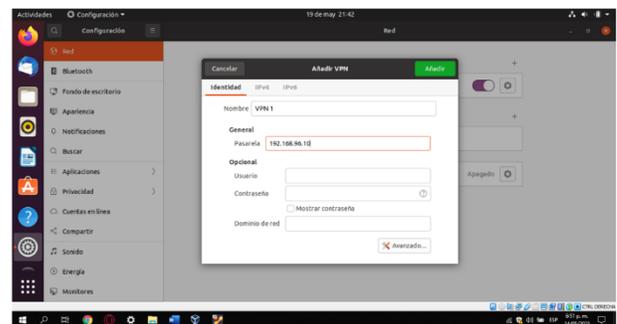


Figura 61. Configuración inicial en cliente.

En configuración avanzada, se selecciona la casilla “Usar cifrado punto a punto (MPPE)”, luego se acepta la configuración y se añade la conexión VPN.

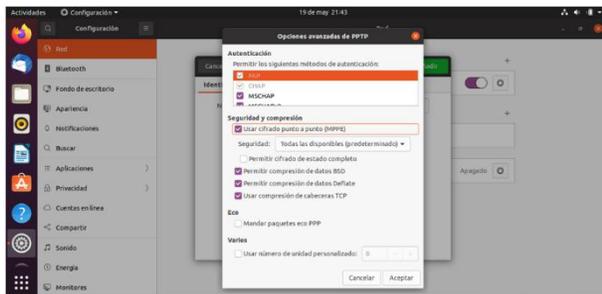


Figura 62. Configuración del cifrado en cliente.

Después de configurar lo anterior se podrá habilitar la conexión VPN.

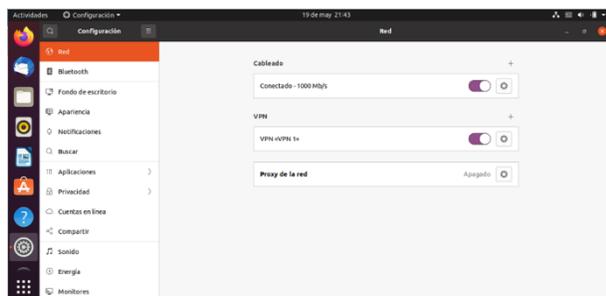


Figura 63. Conexión vpn habilitada en cliente.

Otra forma de demostrar que el servidor VPN se esta ejecutando, es en la Dashboard del servidor Zentyal donde muestra la información de los “Demonios OpenVPN”.

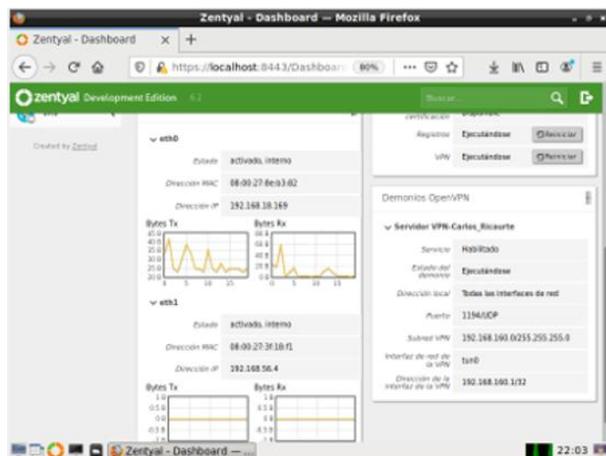


Figura 64. Pruebas de ejecución en la dashboard.

7 CONCLUSIONES

El uso de Zentyal facilitó la administración de redes, a la vez que robustece la seguridad de la misma, permitió establecer parámetros y permisos propios de cada usuario y nivel de grupo de usuarios haciendo que se tenga acceso solamente a la información pertinente para cada uno.

Es importante tener en cuenta la distribución de la red antes de empezar a configurar Zentyal, con el fin de establecer claramente las necesidades de hardware requeridas, y así evitar inconvenientes al poner en marcha los diferentes servicios.

Se aprendió a como instalar y configurar el servidor VPN y en su proceso la configuración inicial de Zentyal. Con la instalación VPN se nos permitió crear conexiones a una red local de manera privada.

El Cortafuegos o Firewall nos brindó muchas alternativas para el filtrado de paquetes tanto de entrada como de salida y todo esto gracias al entorno grafico que posee el servidor Zentyal. Muy buena opción a la hora de implementar redes internas.

8 REFERENCIAS BIBLIOGRÁFICAS

- [1] Zentyal 6.2 Documentación Oficial — Documentación de Zentyal 6.2. (n.d.). Retrieved May 17, 2021, from <https://doc.zentyal.org/6.2/es/>
- [2] Murillo, R. [Roberto Murillo] (16 de mayo de 2020). Zentyal 6.2: Instalación y Configuración - Introducción [Video]. Youtube. https://youtu.be/s5R_Lw3LdYU
- [3] Murillo, R. [Roberto Murillo] (20 de mayo de 2020). Zentyal 6.2: Instalación y Configuración - Parte #1 [Video]. Youtube. <https://youtu.be/gJYJm2vxbc>
- [4] Murillo, R. [Roberto Murillo] (23 de mayo de 2020). Zentyal 6.2: Instalación y Configuración - Parte #2 [Video]. Youtube. https://youtu.be/l-2fw_5BZhs
- [5] Murillo, R. [Roberto Murillo] (28 de mayo de 2020). Zentyal 6.2: Instalación y Configuración - Parte #3 [Video]. Youtube. <https://youtu.be/dKYnY8pZEq>
- [6] Murillo, R. [Roberto Murillo] (3 de junio de 2020). Zentyal 6.2: Instalación y Configuración - Parte #4 [Video]. Youtube. <https://youtu.be/VvYtrP49LCw>
- [7] Murillo, R. [Roberto Murillo] (6 de junio de 2020). Zentyal 6.2: Instalación y Configuración - Parte #5 [Video]. Disponible en. <https://youtu.be/5oU0C3BwSak>
- [8] Zentyal Community. (2015). Servicio de redes privadas virtuales (VPN) con OpenVPN [En línea]. Disponible en: <https://doc.zentyal.org/6.2/es/vpn.html#configuracion-de-un-servidor-openvpn-con-zentyal>
- [9] Perez, B. [Bilmer Perez] (17 de diciembre de 2019). Bloquear facebook con Cortafuegos Zentyal-Server.[Video]. <https://www.youtube.com/watch?v=kHCfxU0Enog>