SOLUCIÓN DE NECESIDADES ESPECÍFICAS EN IT CON ZENTYAL

Lauren Dayana Sanchez
ldsanchez@unad.edu.co
Sebastián Estupiñán Alvarado
sestupinanal@unadvirtual.edu.co
Liliana Andrea Lopez
lalopezvid@unadvirtual.edu.co
Marco Polo caicedo
mpoloca@unadvirtual.edu.co
Anderson Jiménez Torres
ajimenez@unadvirtual.edu.co

RESUMEN: Este trabajo presenta, Soluciones específicas *en el sistema GNU/Linux, y basados en la distribución Zentyal 6.2. En este caso se demuestra la instalación de una máquina virtual, en la cual se ejecutará la distribución, y su respectiva instalación y configuración, teniendo como finalidad la creación y configuración de diferentes herramientas y utilidades del servidor, como es conexión VPN, cortafuegos, DNS y un proxy No Transparente que filtra la salida por medio del puerto 1320.*

Palabras clave: Proxy, No Transparente, DHCP, Distribución, VPN, Cortafuegos.

1 INTRODUCCIÓN

Este trabajo permite aprender y conocer sobre la instalación y manejo del servidor Zentyal, el cual es muy utilizado por las empresas para el control de su tráfico y red virtual, este tiene diferentes utilidades, desde la creación de una red privada, el control de la red con un cortafuegos o simplemente las conexiones privadas entre máquinas mediante un cortafuegos.

2 INSTALACIÓN DE LA MÁQUINA VIRTUAL

Se realiza la configuración preliminar en la máquina virtual, que en este caso es usado el virtual box.

Figura 1. Se Nombra la Maquina

Figura 2. Se establece el valor de la memoria

Figura 3. Configuración disco duro

Figura 4. Tipos de archivos de disco duro

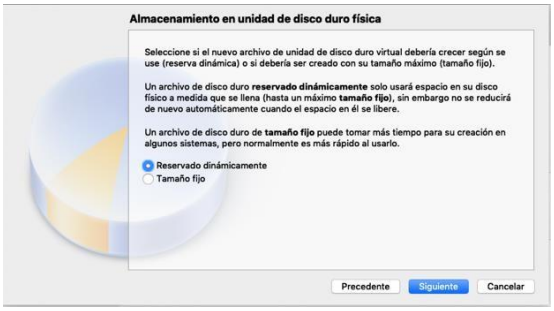


Fig. 5. Se deja en tamaño dinámico el uso del disco duro

Figura 6. Se escoge el tamaño del disco duro

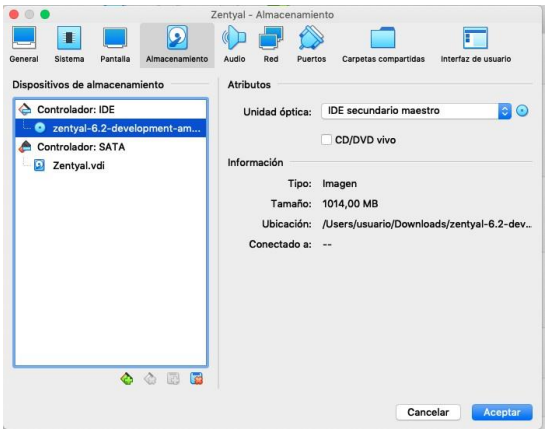


Figura 7. Se selecciona el iso instalador de zentyal.

3 INSTALACIÓN DE LA DISTRIBUCIÓN ZENTYAL 6.2

En este espacio, después de instalada la máquina virtual, se procede a instalar la distribución Zentyal 6.2 a través de la iso descargada.

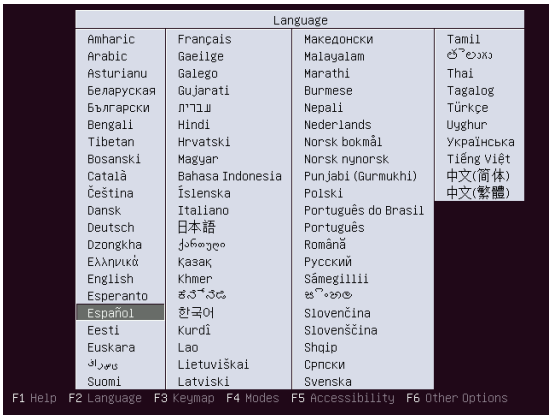


Figura 8. Se escoge el idioma sobre el cual se va a trabajar

Para que inicie la instalación, se solicita borrar todo el disco para que se cargue desde 0.

Figura 9. Se borra el disco

4 TEMÁTICA 1:

DHCP Server, DNS Server y Controlador de Dominio.

Inicio de sesión a Zentyal a través del navegador

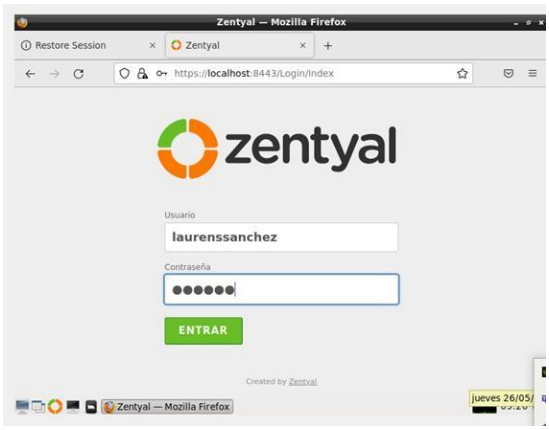


Figura 10. Inicio de sesión en Zentyal

Configuración inicial de los módulos necesarios para desarrollar la implementación de los servicios DHCP Server, DNS Server y Controlador de Dominio. Se seleccionan los servicios Domain Controller and File Sharing, DNS server y DHCP server

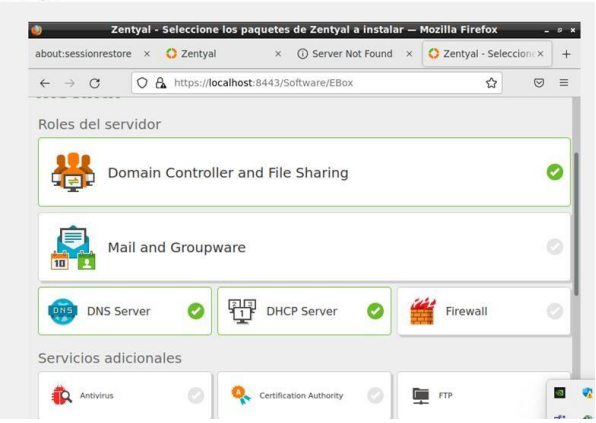


Figura 11. Instalación componentes necesarios

Se confirman los paquetes a instalar

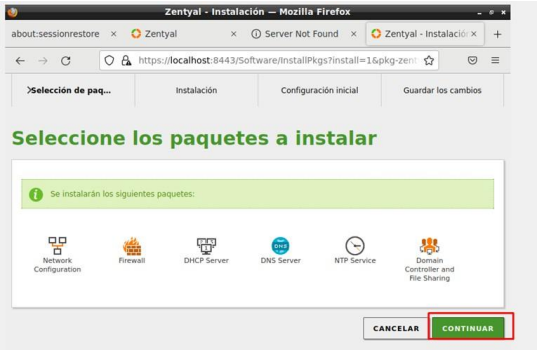


Figura 12. Confirmación instalación componentes

Se configuran las interfaces de red, la interfaz eth0 es la red que tiene salida a internet por lo tanto se marca como External y se configura por método DHCP

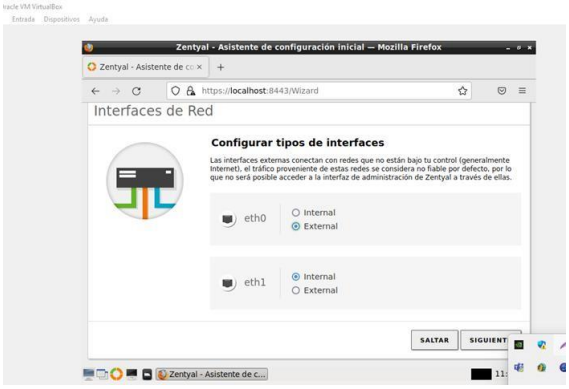


Figura 13. Configuración de interfaces de red

La interfaz eth1 es la red local por medio de la cual se comunicarán los equipos, se configura por método estático y se le asigna la IP 192.168.10.10 para el Zentyal

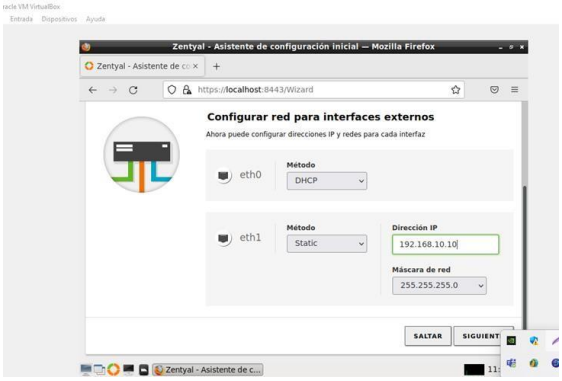


Figura 14. Configuración de interfaces de red

Se selecciona tipo de servidor el cual será Servidor-Stand-Alone y se asigna el nombre del dominio del servidor

Figura 15. Configuración de interfaces de red

Zentyal termina de realizar las configuraciones en el sistema

Figura 16. Finalización configuración componentes

Activación del módulo DHCP en Zentyal

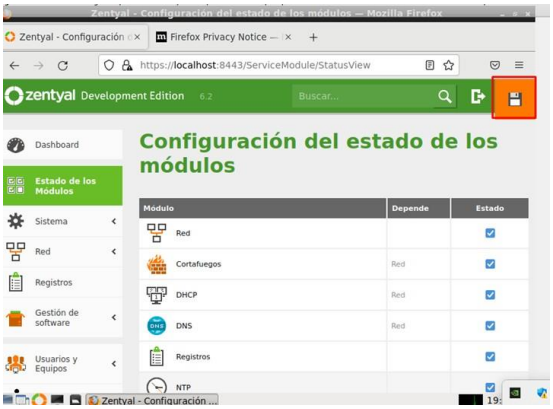


Figura 17. Activación del módulo DHCP

Configuración del servidor DNS, se habilita caché de DNS para forzar el uso del servidor DNS sin realizar cambios en las configuraciones de los clientes y se crean los redireccionadores

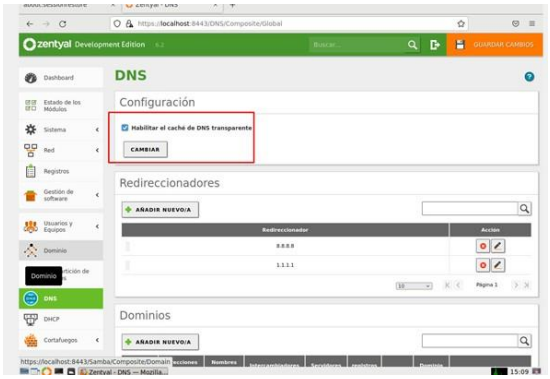


Figura 18. Configuración servidor DNS

Se crea rango de IPS para que el servidor DHCP las asigne en los clientes

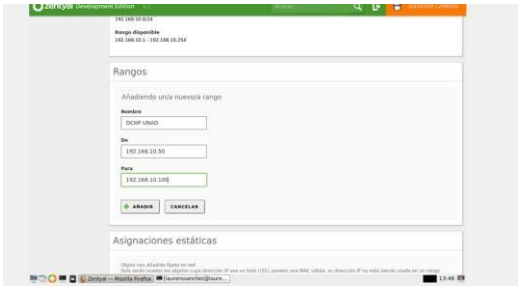


Figura 19. Creación rango de IPS para DHCP.

Se crea usuario administrador para el dominio

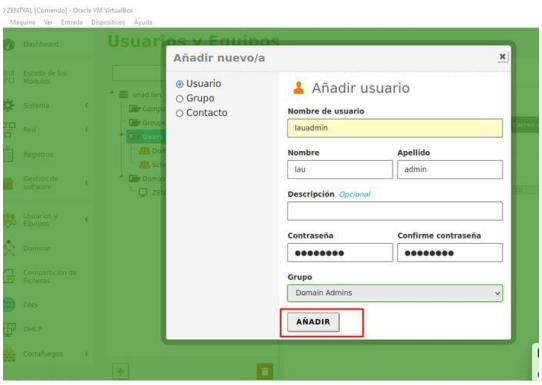


Figura 20. Creación usuario administrador para dominio

Se inicia sesión en equipo cliente Windows y Ubuntu y se valida que el servidor DHCP asigna las IPS a los clientes en el rango especificado.

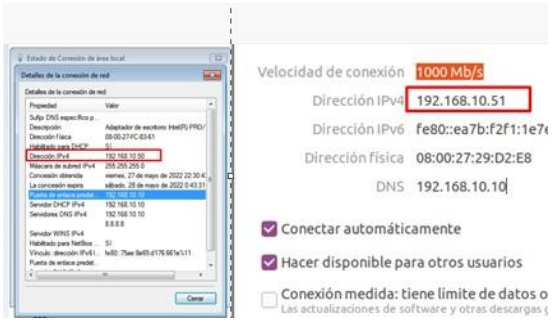


Figura 21. Verificación servidor DHCP en clientes

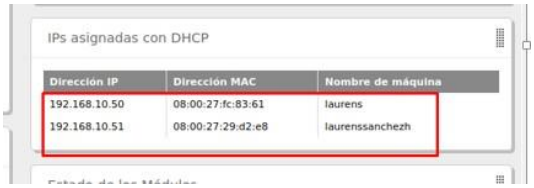


Figura 22. Verificación IPS asignadas desde Zentyal

Se agrega el cliente Windows al dominio unad.lan

Figura 23. Cliente Windows agregado al dominio

Instalación de pbis en Ubuntu para unir este cliente al dominio

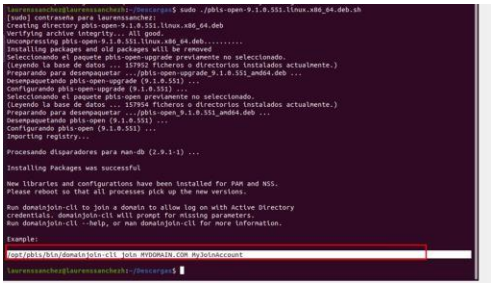


Figura 24. Instalación pbis en Ubuntu

Se ejecuta comando para unir cliente Ubuntu al dominio unad.lan

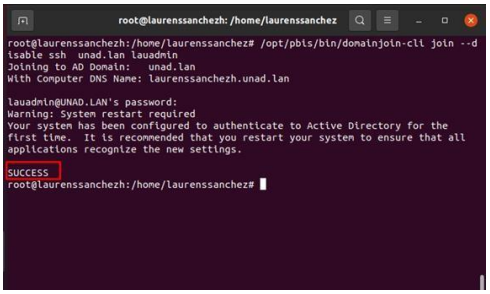


Figura 25. Instalación pbis en Ubuntu

Se verifica en Zentyal que los clientes hacen parte del dominio

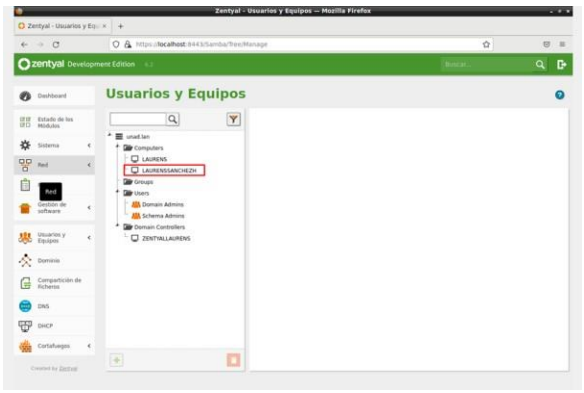


Figura 26. Clientes en el dominio unad.lan

5 TEMÁTICA 2:

Proxy no transparente el Proxy transparente, se entiende como el servicio que se usa para la protección de las IP verdaderas, y sobre el cual se debe realizar la modificación en el equipo cliente y en el navegador usado.

Configuración proxy no transparente en el zentyal: Se Inicia el sistema Zentyal, donde pide el usuario y la contraseña

Figura 27. Inicio del Zentyal

Al ingresar con usuario y contraseña se puede realizar una configuración Inicial, en donde se eligen qué servicios se instalarán.

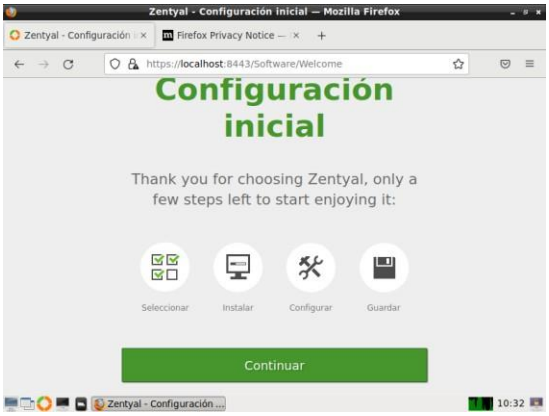


Figura 27. Configuración Inicial.

Se eligen los servicios que se quieren instalar, son los señalados por el símbolo de Ok verde.

Figura 28. Instala servicios

Al solicitar los servicios, se pide instalar paquetes necesarios para su uso.

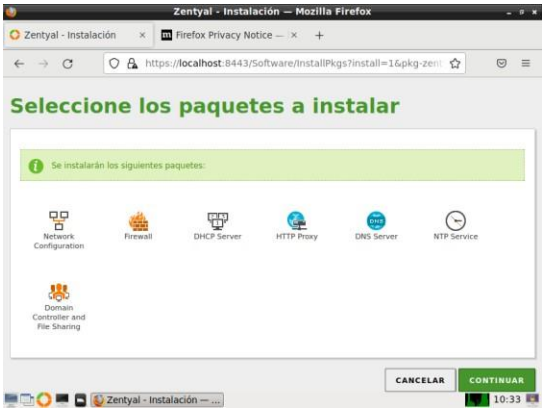


Figura 29. Instala paquetes

Figura 30. Instala paquetes

Pide configurar dos redes, una externa y una interna.

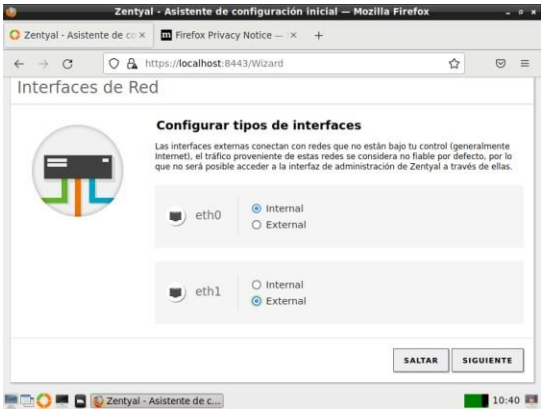


Figura 31. Configuración de Red

Se configura la red estática, con el ip sobre el cual se encuentra el servidor, para este caso la IP estática será 192.168.0.106 con la máscara 255.255.255.0

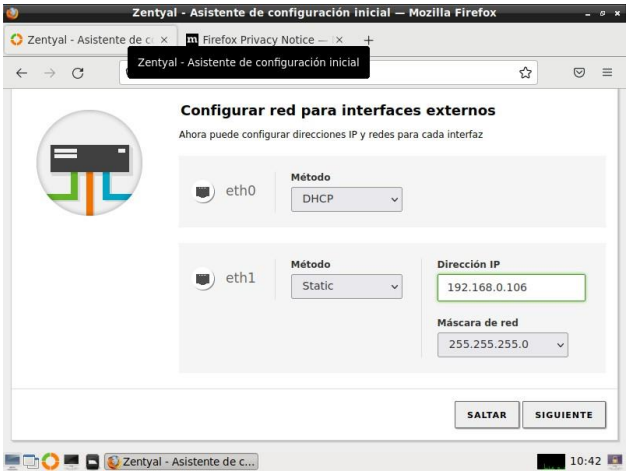


Figura 32. Configuración de IP

Se selecciona el tipo de servidor que en este caso será Stand-alone o independiente y se define el dominio que por defecto lo trae como zentyal-domain.lan

Figura 33. Servidor Stan-alone y dominio

En este paso después de instalado y configurado los pasos anteriores, se ingresa a la pestaña de Proxy http y en configuraciones generales, se referencia como proxy no transparente, dejando la opción seleccionada y se cambia el puerto, por el puerto solicitado, que en este caso es el 1320

Figura 34. Configuración Proxy No Transparente y Puerto

Se Guardan los cambios realizados en la configuración Proxy No Transparente

Figura 35. Guardando Cambios

Se edita la regla, que en este caso deniega todo ingreso a internet.

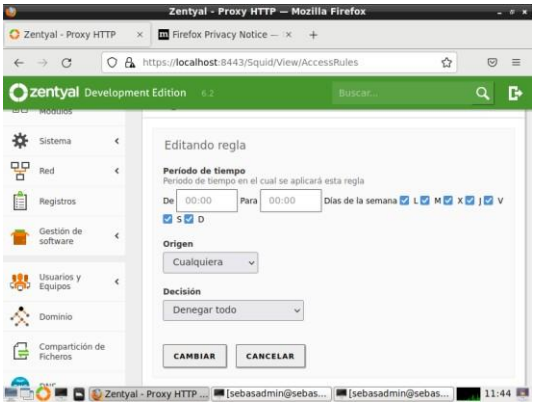


Figura 36. Edita Regla

Se realiza el proceso de configuración y visualización en Ubuntu desktop.
Se comprueba que en Ubuntu esté funcionando el internet correctamente. En este caso se ingresa una página de Youtube.

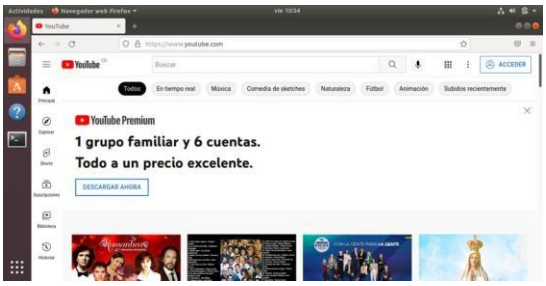


Figura 37. Comprobación de Acceso a Internet desde Desktop página de Youtube.

En las opciones de red del Desktop de configurar la dirección IP del servidor, que será el proxy

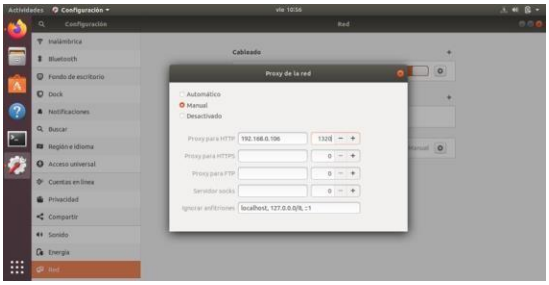


Figura 38. Configuración de Proxy en el Desktop.

En las configuraciones de Internet del Mozilla Firefox, se realiza la configuración de Proxy Manual, por ser un proxy No Transparente.

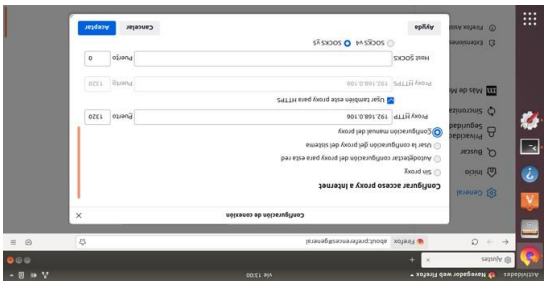


Figura 39. Configuración de Proxy en el Mozilla Firefox

Se Ingresa Nuevamente al Browser de Firefox para comprobar si el Proxy está surtiendo efecto y efectivamente, no permite el ingreso a la página de Youtube, por la ejecución del Proxy.

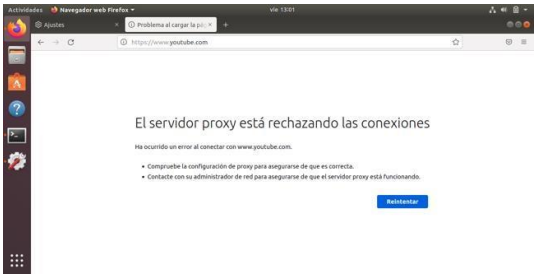


Figura 40. Comprobación del cargue de la página de Youtube.

6 TEMÁTICA 3: CORTAFUEGOS

El cortafuegos es un sistema de seguridad para bloquear accesos no autorizados a un ordenador mientras sigue permitiendo la comunicación del ordenador con otros servicios autorizados, en este caso se va a denegar el acceso a páginas de redes sociales, esta validación se hará desde el usuario desktop

Figura 41. Autenticación en el servidor

Para la interfaz wan se va dejar por DHCP, para la red Lan se usará una ip estática 192.168.10.1

Figura 42. Configuración interfaces

Para definir las reglas que conforman la política de un cortafuego se hará uso de los los Servicios de red para especificar a qué protocolos y puertos se aplican las reglas y también de los objetos de red para especificar sobre qué direcciones IP de origen o de destino a las que se aplican. Se crea 2 objetos uno para los usuarios de la red lan y otro donde se agruparán las ip de las páginas a bloquear.

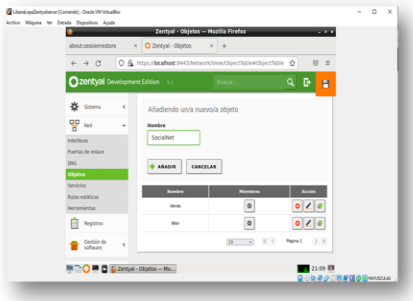


Figura 43. Creación SocialNet

En los miembros se especifica los rangos de ip que se desea bloquear

Figura 44. Se añade a Facebook

Antes de la implementación, se tiene acceso correcto desde el usuario desktop a Facebook.

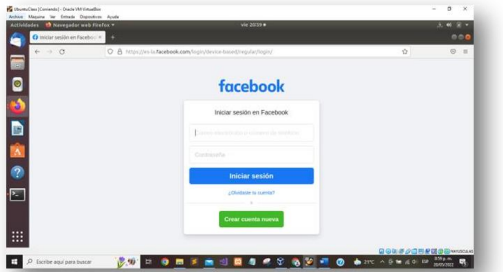


Figura 45. acceso correcto a Facebook

Se adicionan en los miembros, los rangos de ip de las redes sociales (instagram, twitter,whatsapp).

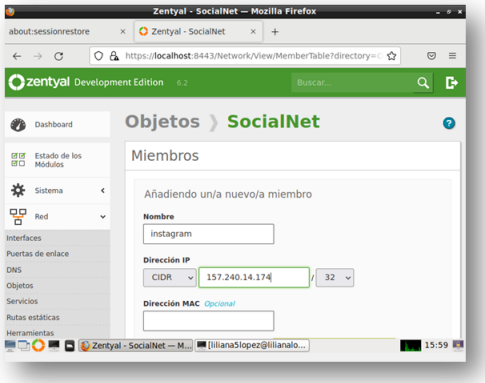


Figura 46. Se añade Instagram

Figura 47. Acceso correcto a Instagram

Después de añadir todos los miembros, se procede a guardar los cambios.

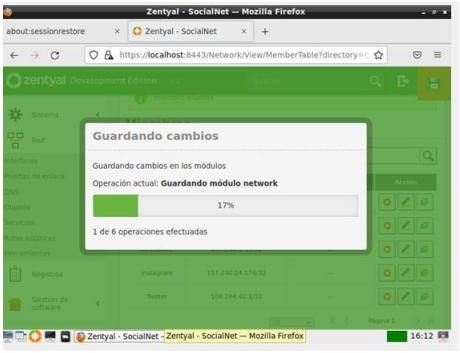


Figura 48. Se guardan los cambios

Posteriormente se crea una regla para el filtrado de los paquetes especificando los protocolos y puertos, para esto se procede a crear un servicio el cual incluirá el protocolo TCP/UDP con puerto de destino 443.

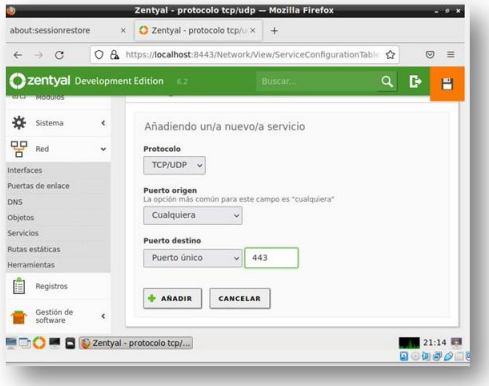


Figura 48. creación servicio

Se crea la regla que deniegue el servicio TDC/UDP de cualquier origen al objeto Socialnet

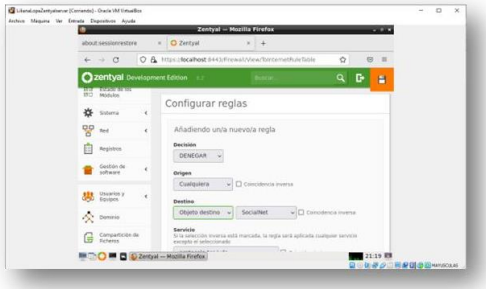


Figura 49. creación regla

Se valida que las reglas se hayan implementado y bloqueen el acceso a las redes sociales del usuario desktop.

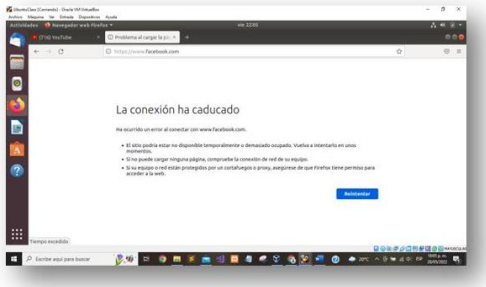


Figura 50. validación acceso denegado a Facebook

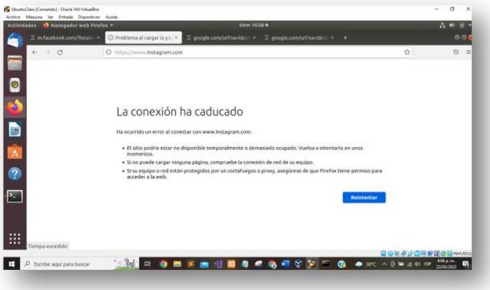


Figura 51. validación acceso denegado a Instagram

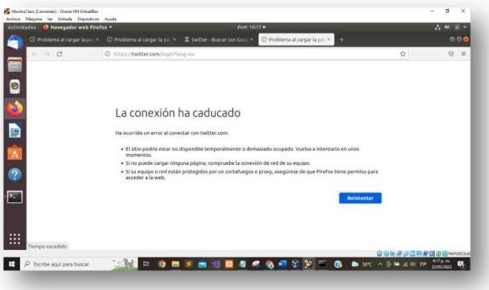


Figura 52. validación acceso denegado a twitter

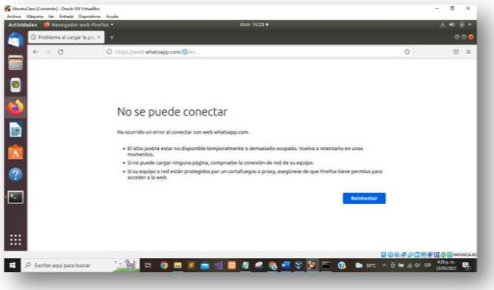


Figura 53. validación acceso denegado a whatsapp

Se verifica conexión correcta a otras páginas.

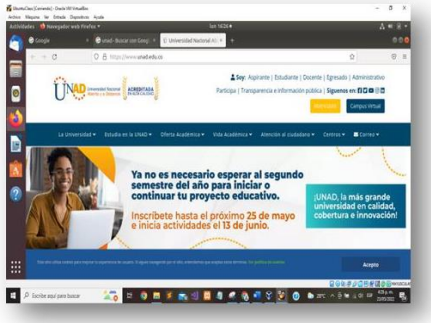


Figura 54. Validación acceso correcto a la página de la unad

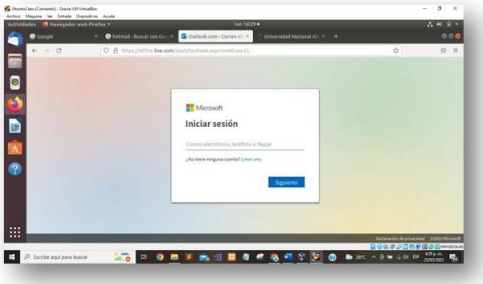


Figura 55. validación acceso correcto a Hotmail.

7 TEMÁTICA 4:

File Server y Print Server Configuración de módulos.

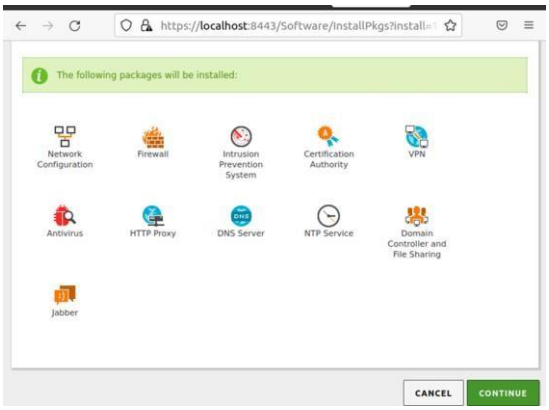


Figura 56. FS y PS módulos.

Sección de usuarios y equipos.

Figura 57. FS y PS usuarios equipos.

Creación de grupos.

Figura 58. FS y PS grupos.

Grupo de administración creado. Propiedades y configuración del usuario administrador.

Figura 59. FS y PS nuevo usuario.

Creación de un nuevo usuario (marco), asignado al grupo administración.

Figura 60. FS y PS agregar usuario a grupo.

Configuramos el rango en DHCP

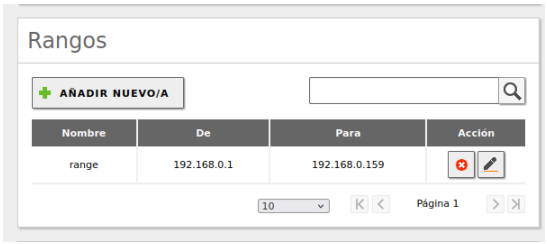


Figura 61. FS y PS rango dhcp.

Creación de un fichero para ser compartido.

Figura 62. FS y PS fichero.

Ficheros creados, para ser compartidos.

Figura 63. FS y PS compartir ficheros.

Damos clic en añadir para Configurar el fichero prueba.

Figura 64. FS y PS añadir ficheros.

Propiedades y control del fichero final

.

Figura 65. FS y PS fichero unad final.

Ingresamos al archivo resolv.conf, para modificar la ip de acceso.

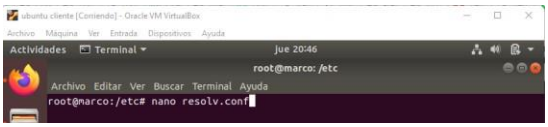


Figura 66. FS y PS resolvconf.

Agregamos la ip de nuestro servidor.

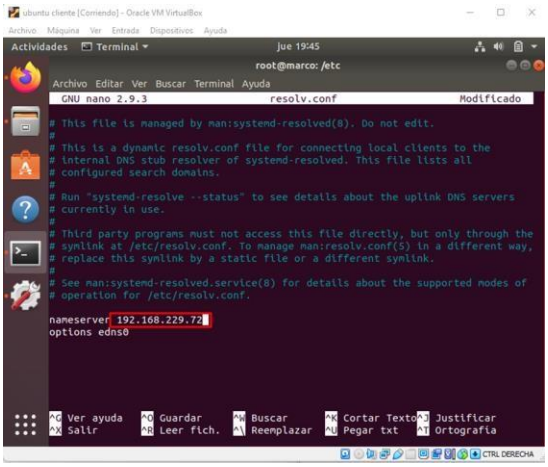


Figura 67. FS y PS ip servidor.

Instalamos en Ubuntu unas aplicaciones que nos permitirán crear el enlace. pbis-open

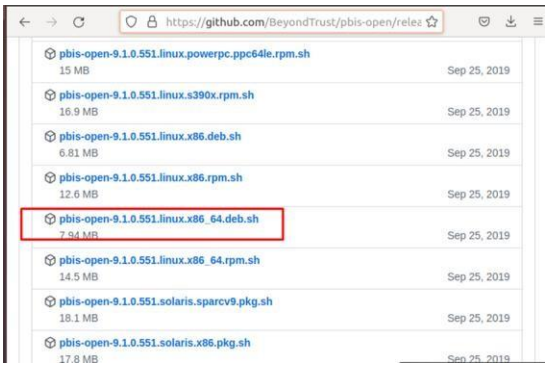


Figura 68. FS y PS instalar en ubuntu.

Con el comando sudo domainjoin-gui abrimos para la conexión. La aplicación reconoce el nombre de la máquina, agregamos el dominio. Nos autenticamos con el usuario de zentyal.

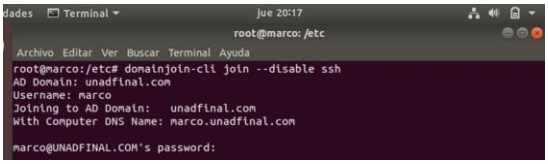


Figura 69. FS y PS autenticación.

8 TEMÁTICA 5:

VPN El servidor zentyal permite la creación de una red privada para el manejo de una red interna. Para utilizar esta utilidad del servidor se deben seguir los siguientes pasos:

Después de instalar el servidor seleccionar las utilidades de:

- Cortafuegos
- Certificados
- Red
- VPN

Podremos comenzar a crear todo para la red privada.

Primero se debe crear un certificado para utilizarlo en el servidor VPN. Para ello se debe ir a la sección de certificados, asignar un nombre y un tiempo de expiración:

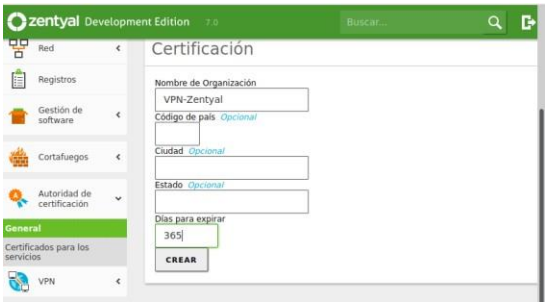


Figura 70. Creación certificada para VPN

Se debe verificar la creación del certificado, finalmente se debe ver así la tabla de certificados:

Figura 71. Tabla de certificados

Paso seguido se debe ingresar a la sesión del menú VPN, allí se debe seleccionar servidores, crear un nuevo servidor. Para esto se asigna un nombre y se da clic en crear y guardar.

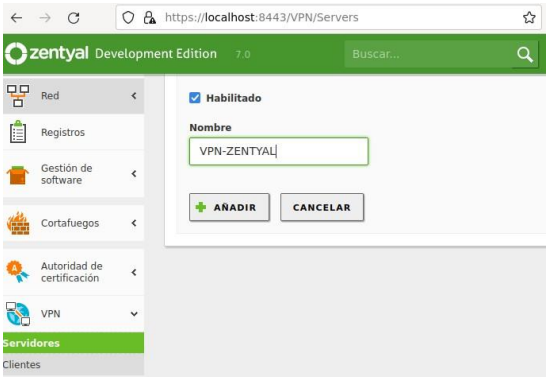


Figura 72. Creación certificada para VPN

Posteriormente se debe dar clic en configurar el servidor, allí se deberá asignar la dirección de red, el certificado de seguridad para la conexión VPN, así como otras configuraciones.

Figura 73. Tabla de servidores VPN

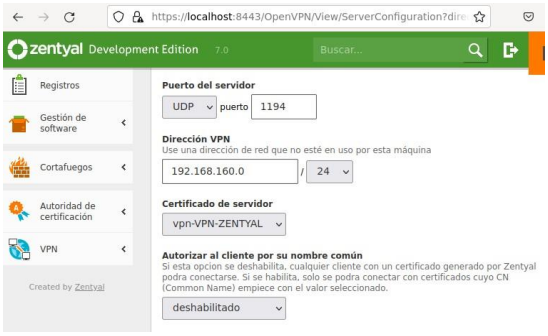


Figura 74. Creación de servidor VPN

Creación de servicio VPN: En el menú, ingresar a la sesión de servicios que se encuentra en la red, allí se debe proceder a crear un nuevo servicio, seguido de la asignación del protocolo a utilizar y el puerto de entrada y destino.

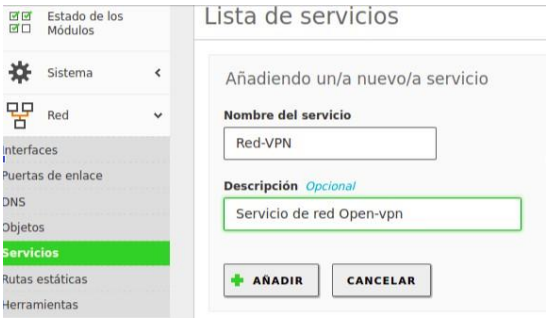


Figura 75. Creación de servicio conexión VPN

Figura 76. Configuración servicio VPN

Después de la configuración el servicio se deberá ver así:

Figura 77. Tabla de servicios.

Paso seguido después de la configuración del servicio, es agregar este servicio como una regla del firewall, esto permitirá que al conectarse un cliente vía VPN, el firewall le conceda acceso por el puerto especificado, en esta ocasión es el 1194.

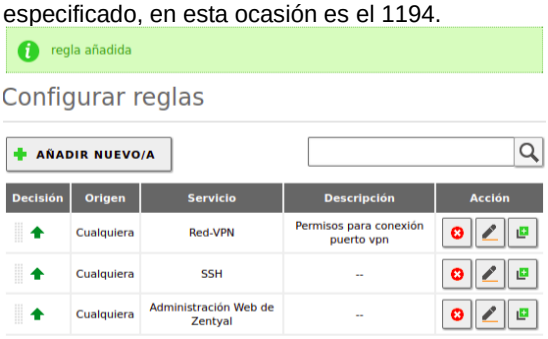
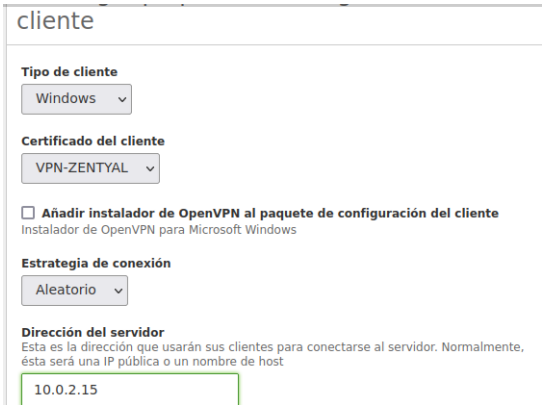


Figura 78. Tabla de reglas en el cortafuegos

Finalmente se deberá ingresar de nuevo a la sección de VPN, se deberá descargar el cliente VPN, asignando la puerta de enlace de nuestro proveedor de red y también la dirección IP del servidor.



Con esto realizado, se debe descargar el openvpn cliente y con lo que se descargó del servidor Zentyal realizar la conexión a la red privada.

9 CONCLUSIONES

Se realizó instalación de paquetes para realizar la asignación de direcciones IP automáticamente por el server DCHP, de igual forma se realiza configuración de los DNS para permitir el acceso a la web en equipos clientes y se realiza configuración de dominio y se agregan equipos a este, por medio de este laboratorio se obtienen conocimientos en el manejo de la herramienta Zentyal y su configuración.

Sobre el sistema se pudo comprobar los pasos necesarios para su correcta instalación y puesta en marcha, la cual permitió crear el proxy No transparente. ·

Se Implementa y configura un cortafuegos sobre la distribución Zentyal Server lo que facilita tener un control de seguridad perimetral sobre la red de la empresa.

Al implementar y configurar el servidor Zentyal se puede lograr crear un dominio para el ingreso a las carpetas.

El servidor zentyal es una gran opción inicial para una empresa pequeña que está empezando, con este podemos configurar una red privada mediante una vpn y restringir accesos específicos mediante el firewall.

10 REFERENCIAS

[1] Zentyal 6.2 (s.f.) ” Configuración de un servidor de dominio con Zentyal”, Documentación de Zentyal 6.2. [En línea]. Disponible en: https://doc.zentyal.org/6.2/es/directory.html#configuracion-de-un-servidor-de-dominio-con-zentyal

[2] Zentyal 6.2 (s.f.),” Servicio de Proxy HTTP”, Documentación de Zentyal 6.2. [En línea]. Disponible en: https://doc.zentyal.org/6.2/es/proxy.html#configuracion-general-del-proxy-http-con-zentyal

[3] Cortafuegos. (2021). Zentyal Community.[En línea]. Disponible en: https://doc.zentyal.org/es/firewall.html

[4] Youtube - Zentyal - Configuraciones iniciales de Red, DNS y Dominio [Video] Tomado de: https://www.youtube.com/watch?v=3pVd3a1utZo

[5] Zentyal 6.2 Documentación Oficial. (2018). Zentyal Community.[En línea]. Disponible en: https://doc.zentyal.org/6.2/es/