IMPLEMENTACIÓN DE SERVICIOS DE GESTIÓN DE INFRAESTRUCTURA TI SOBRE ZENTYAL SERVER

Cristian David Baquero Ruiz
e-mail: cdbaqueror@unadvirtual.edu.co
Camilo Ernesto Chaparro Penagos
e-mail: cechaparrop@unadvirtual.edu.co
Lady Paola Cuevas Triviño
e-mail:lpcuevast@unadvirtual.edu.co
Julie Marcela Gutiérrez Pacheco
e-mail:jmgutierrezpa@unadvirtual.edu.co
Jorge Enrique Duque Escobar
e-mail: jeduquees@unadvirtual.edu.co

RESUMEN: *El presente informe busca evidenciar la descarga, instalación y configuración del servidor zentyal server como SO base, con la finalidad de realizar la implementación y despliegue de los servicios para gestión de infraestructura TI, a saber, DHCP server, DNS server, controlador de dominio, Proxy no transparente, Firewall, File & Print server, y VPN, para ello, cada integrante del grupo seleccionó una de las temáticas abordadas en el desarrollo del paso 8, a continuación, cada uno creó una nueva máquina virtual, en la que se realizó la instalación y configuración zentyal server como SO base. Una vez realizada la instalación, y previa elección de la temática, se procedió a la instalación y configuración de los módulos base necesarios para realizar la implementación de dichos servicios, una vez instalados y configurados los módulos, como resultado, se procede a dar respuesta a las solicitudes planteadas en el caso de estudio para cada temáticas.*

PALABRAS CLAVE: Zentyal server, DHCP, DNS, proxy, firewall, file & print server, vpn.

ABSTRACT: *This report aims to demonstrate the download, installation and configuration of zentyal server as the base OS, in order to implement and deploy the services for IT infrastructure management, namely DHCP server, DNS server, domain controller, non-transparent proxy, Firewall, File & Print server, and VPN, for this, each member of the group selected one of the topics addressed in the development of step 8, then, each created a new virtual machine, in which the installation and configuration of zentyal server as base OS was performed. Once the installation was done, and after choosing the topic, the base modules needed to implement these services were installed and configured. Once the modules were installed and configured, as a result, we proceeded to respond to the requests raised in the case study for each topic.*

KEY WORDS: Zentyal server, DHCP, DNS, proxy, firewall, file & print server, vpn.

1 INTRODUCCIÓN

En el mundo de las distribuciones Linux existen muchas herramientas que permiten adaptar la infraestructura IT según las necesidades de la empresa, haciendo de la administración del sistema un proceso menos complejo y costoso. Dentro de estas herramientas encontramos Zentyal Server que contiene un paquete de programas para la gestión de la infraestructura de red, permitiendo así la configuración de los diversos servicios que necesita la empresa.

Zentyal server, es un servidor de linux completo que comprende los diferentes servicios tales como DHCP, DNS, Compartición y controlador de archivos, FTP, VPN, Firewall, o mail entre otros, además es software libre. Es una herramienta que nos permite instalar, configurar y administrar los diferentes servicios que su completa oferta nos permite trabajar. Mediante el desarrollo de la presente actividad, se realizará la implementación de servicios de infraestructura TI para intranet y extranet, por medio de servicios como DHCP, DNS, y controlador de dominio, Proxy, Cortafuegos, File & print server, y VPN.

2 SELECCIÓN DE TEMÁTICAS

Tabla 1. Selección de temáticas

Integrante	Temática
Cristian Baquero	1. DHCP Server, DNS Server y Controlador de Dominio
Julie Marcela Gutierrez	2. Proxy no transparente
Camilo Chaparro	3. Cortafuegos
Jorge Enrique Duque	4. File Server y Print Server
Lady Paola Cuevas	5. VPN

3 INSTALACIÓN ZENTYAL SERVER

Creamos una nueva máquina virtual, insertamos la imagen ISO descargada en el almacenamiento, y la iniciamos. Lo primero que seleccionamos es el idioma.

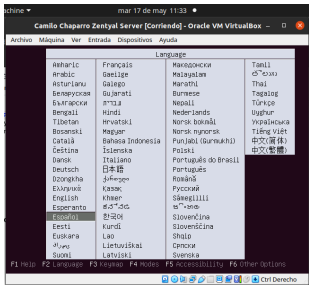

Figura 1. Selección de idioma

En seguida, seleccionamos el método de instalación.

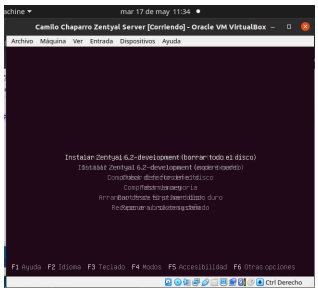

Figura 2. Selección del método de instalación

Seleccionamos el país de ubicación

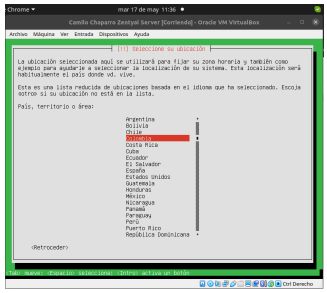

Figura 3. País de instalación

A continuación seleccionamos la distribución del teclado.

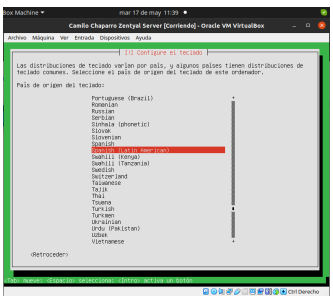

Figura 4. Distribución del teclado

Seleccionamos la interfaz de red primaria

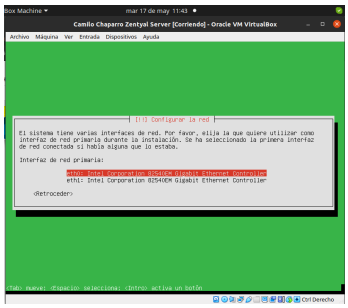

Figura 5. Selección interfaz de red primaria

Enseguida se le da nombre a la máquina

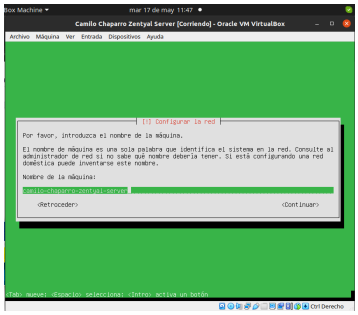

Figura 6. Nombre de la máquina

Ahora creamos el usuario, primero seleccionamos un nombre de usuario.

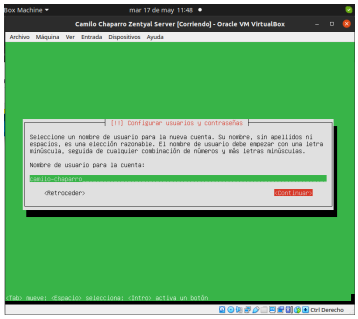

Figura 7. Nombre de usuario

Ahora se selecciona una contraseña y se confirma.

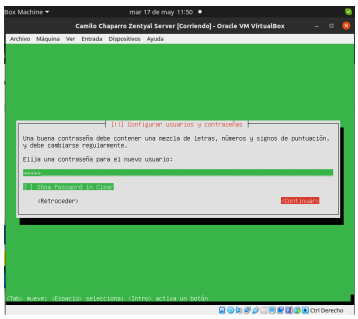

Figura 8. Contraseña de usuario

En seguida se confirma la zona horaria

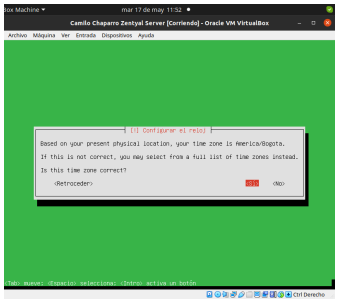

Figura 9. Confirmación zona horaria

Ahora, se particiona, se formatea el disco, se instala el sistema, se configuran los repositorios, se seleccionan e instalan los programas, se instala el cargador de arranque.

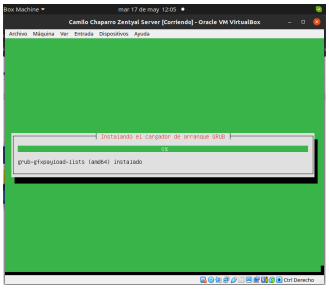

Figura 10. Proceso de instalación

De esta forma finaliza el proceso de instalación, ahora se reinicia, y nos solicita retirar el medio de instalación.

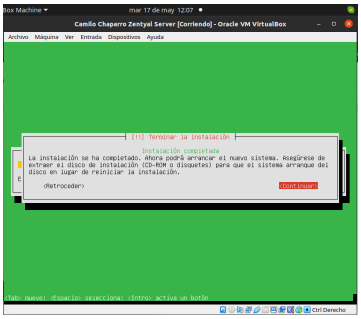

Figura 11. Finalización de instalación

Una vez se reinicia el sistema, carga la interfaz web, e ingresamos con usuario y contraseña.

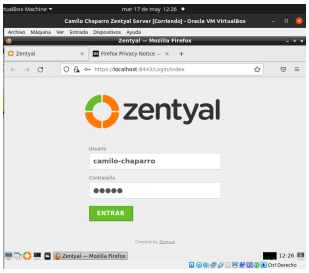

Figura 12. Login

Una vez nos logueamos, realizamos la configuración inicial.

Figura 13. Configuración inicial

4 TEMÁTICA 1. DHCP SERVER, DNS SERVER Y CONTROLADOR DE DOMINIO

Se debe escoger los roles que se desean instalar, en el caso del laboratorio se selecciona Domain Controller, DNS Server, DHCP

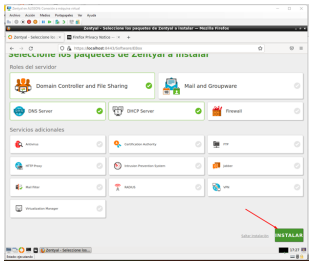

Figura 14. Configuración roles

El sistema muestra un resumen de los paquetes que requiere instalar y solicita una confirmación

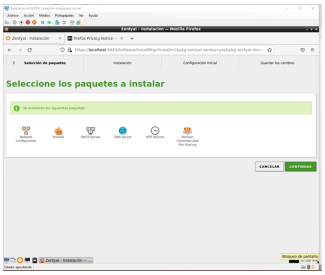

Figura 15. Confirmación roles

Luego de instalar los paquetes necesarios se deben configurar las interfaces de red, en este caso la interface eth0 funciona como WAN y se encuentra en DHCP ya que el operador de internet entrega direcciones por este protocolo, la interfaz eth1 funciona como la puerta de enlace y entregará DCHP a los equipos pertenecientes a la red de zentyal

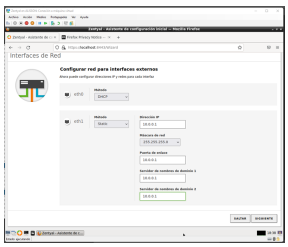

Figura 16. Configuración interfaces de red

Luego se procede a configurar el servidor de Dominio, como es el primer controlador de dominio en la red se realiza una configuración Stand Alone, para efectos del laboratorio como nombre del dominio se asigna el nombre zentyal-domain.lan

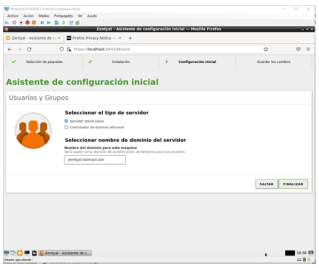

Figura 17. Configuración Domain Controller

El sistema muestra esta pantalla para anunciar que ya se terminó la configuración inicial

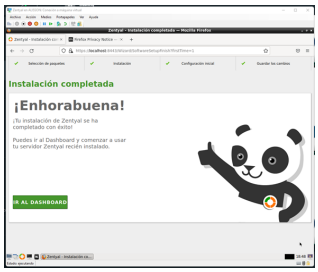

Figura 18. Confirmación instalación

Dentro de la configuracion de modulos se puede ver que modulos estan activos

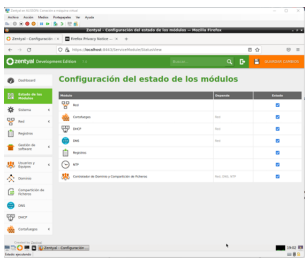

Figura 19. Resumen Roles Activos

Dentro de los servicios se realiza la configuración del DHCP, el pool que se asigna es desde la dirección 10.0.020 hasta la dirección 10.0.0.100

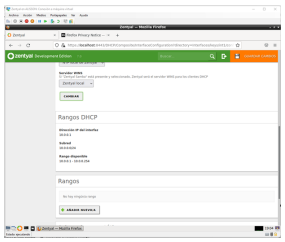

Figura 20. Configuración DHCP paso 1

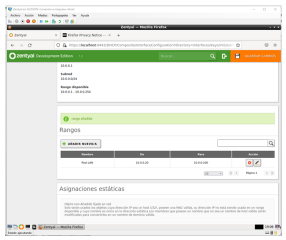

Figura 21. Configuración DHCP paso 2

Ya con estas configuraciones se podrán conectar equipos a la interfaz eth1 la cual les asignará una dirección ip dentro del rango del pool configurado, en este caso se puede evidenciar que la ip asignada al equipo preparado para ser subido al dominio es la 10.0.0.21

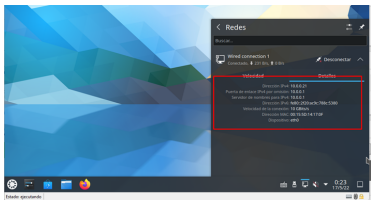

Figura 22. Asignación DHCP

Para unir el equipo Linux al dominio se requieren ejecutar e instalar varios paquetes desde la consola, con el fin de facilitar esto se realiza conexión vía ssh,

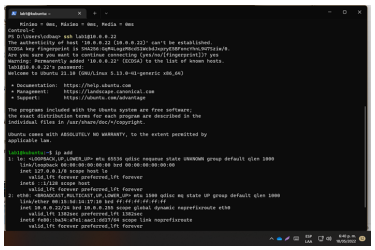

Figura 23. Conexión vía SSH

Se descarga AD Bridge Open, desde el repositorio oficial en GitHub de acuerdo con la versión del sistema, en este caso pbis-open-9.1.0.551.linux.x86_64.deb.sh

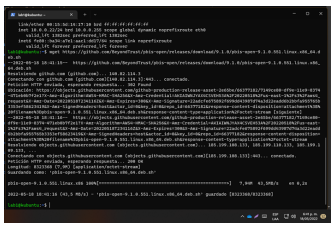

Figura 24. Descarga AD Bridge

Para poder ejecutarlo se otorgan permisos con el comando chmod y el nombre del archivo descargado

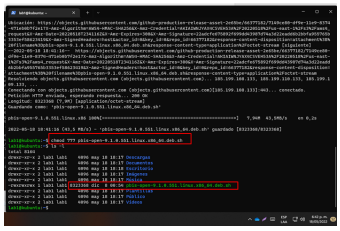

Figura 25. Permisos AD Bridge

Se ejecuta sudo ./pbis-open-9.1.0.551.linux.x86_64.deb.sh para instalar el paquete requerido, finalizada la instalación muestra un ejemplo de ejecución en consola

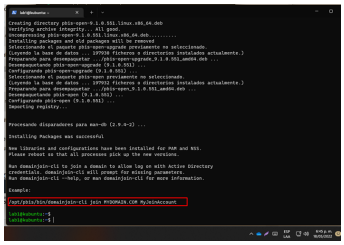

Figura 26. Ejecución instalación AD Bridge

Se ejecuta el comando indicando el dominio y el usuario con el que se requiere hacer login, el usuario debe pertenecer a los administradores de dominio para lograr la integración a este

Figura 27. Instalación completa AD Bridg

El sistema indicará que es necesario hacer un reinicio de la máquina para completar la operación

En la ventana de administración se puede validar el nuevo equipo en la carpeta de Computers

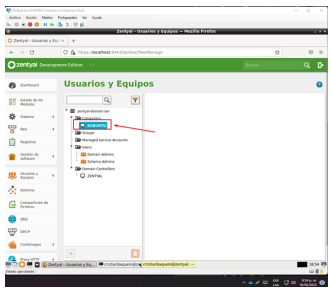

Figura 28. Registro Maquina en Domain Controller

Se valida en la consola del equipo ejecutando el comando hostname

Figura 29. Registro Hostname en Domain Controller

Para realizar la prueba de inicio de sesión en el equipo, se realiza la creación de un usuario de prueba

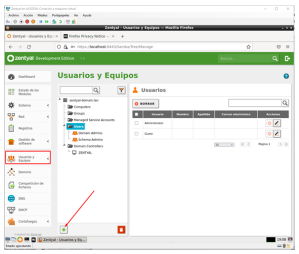

Figura 30. Creación usuario

Se valida el usuario creado

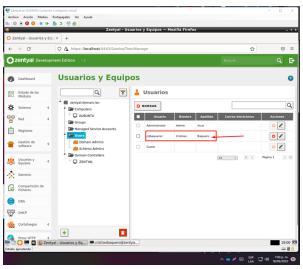

Figura 31. Validación usuario

Se realiza inicio de sesión con el usuario creado indicando el dominio y la contraseña asignada

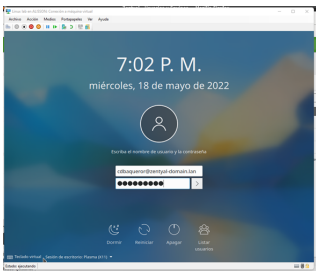

Figura 32. Inicio sesion usuario dominio

Validación del usuario dentro del escritorio

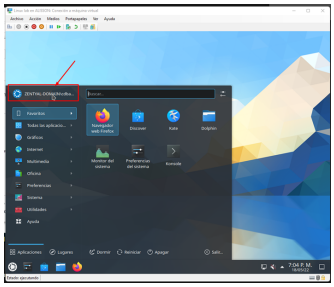

Figura 33. Validación Usuario desde info de usuario

Validación de las carpetas en /home

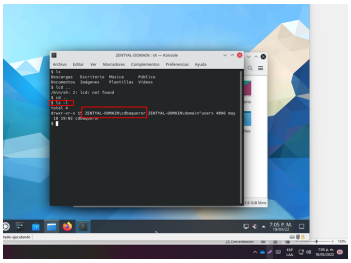

Figura 34. Validación Usuario desde /home

5 TEMÁTICA 2. PROXY NO TRANSPARENTE

El Servidor Proxy NAT o proxy no-transparente, es un servicio proxy que se usa principalmente para proteger la identidad de las verdaderas conexiones IP que acceden a Internet.

Ingresa a estados de módulos y seleccionamos Proxy HTTP.

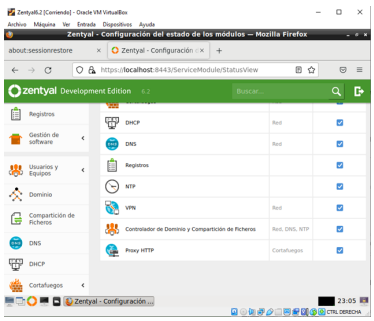

Figura 35. Proxy HTTP.

Deshabilitamos Proxy transparente y colocamos el puerto 1320.

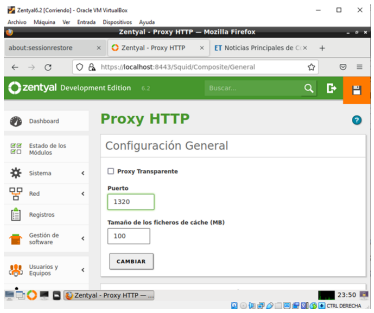

Figura 36. Puerto 1320.

Una vez realizada la parte de configuración se selecciona perfiles de filtro y se da crear uno.

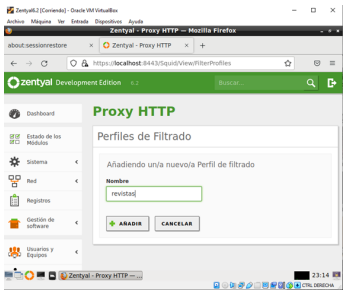

Figura 37. Perfil de filtrado.

Configuramos el umbral de filtrado de qué tan estricto requerimos la regla de filtrado.

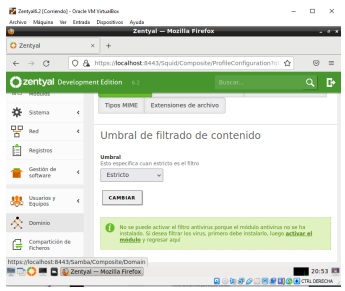

Figura 38. Perfil de filtrado.

Añadimos una regla de dominio para denegar el acceso a una página.

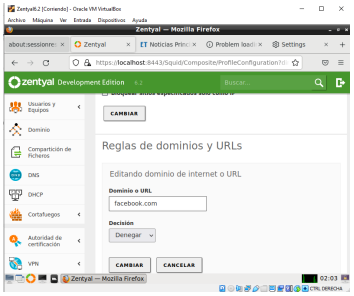

Figura 39. Bloqueo URL.

Vamos a las reglas de acceso en Proxy y creamos una.

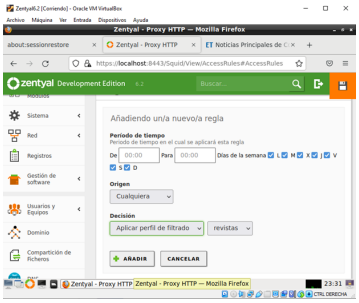

Figura 40. Reglas de acceso.

Nos vamos a la máquina cliente y configuramos la IP y puerto del proxy configurado en Zentyal y probamos el acceso a la página de bloqueada facebook. En el navegador del cliente en configuración avanzada ingresamos el proxy manual.

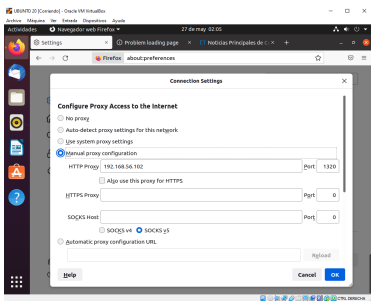

Figura 41. Ingreso Proxy en el navegador.

Verificamos que no abra la página. El proxy está funcionando y está bloqueando la navegación en el equipo

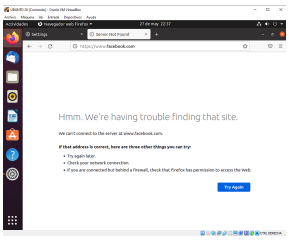

Figura 42. Proxy bloqueado.

6 TEMÁTICA 3. CORTAFUEGOS

Para iniciar, se va a hacer uso del siguiente direccionamiento de red:

WAN: DHCP	Gateway: 10.0.0.1
LAN: 10.0.0.0	Zentyal: 10.0.0.2
Máscara de red: 255.255.255.0	Pool: 10.0.0.5 - 10.0.0.254

Dicho lo anterior, en primer lugar, se va a realizar la configuración inicial, para ello, se van a seleccionar los paquetes a instalar, en este caso cortafuegos

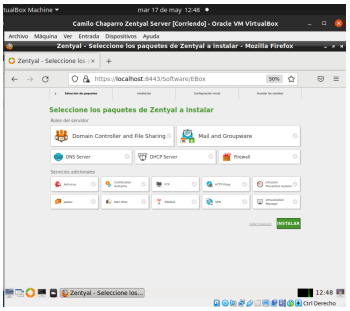

Figura 43. Selección de paquetes a instalar

Al realizar la selección de paquetes, Zentyal muestra un resumen de los paquetes adicionales a instalar.

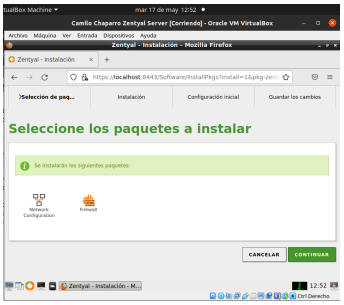

Figura 44. Paquetes adicionales

Luego de que se instalan los paquetes, se procede a configurar los tipos de interfaces, en este caso una externa y una interna.

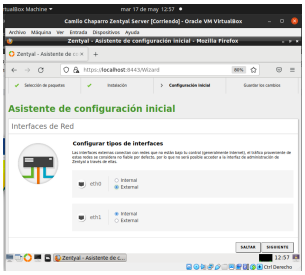

Figura 45. Configuración tipos de interfaces

A continuación se configuran las direcciones ip para cada interfaz, cuando el método es estático, se debe ingresar la máscara de red.

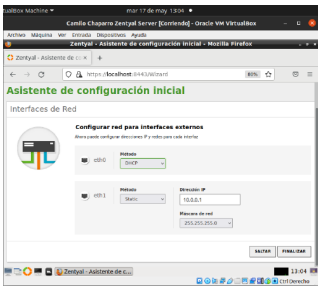

Figura 46. Configuración direcciones ip interfaces

A continuación, se guardan los cambios realizados y se completa la instalación del servicio.

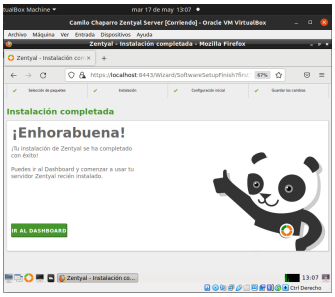

Figura 47. Finalización instalación de servicio

En el paso anterior, se configuraron las direcciones ip para cada interfaz, ahora, se deben verificar/ configurar las puertas de enlace o gateways.

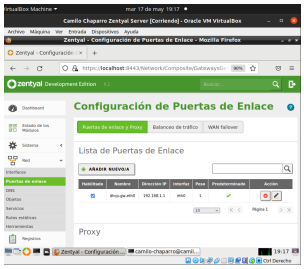

Figura 48. Verificación / configuración puertas de enlace

Ahora se configura el traductor de servidores de nombre de dominio, se agregan los servidores de google por defecto, y se verifica que la puerta de enlace también se encuentra en esta configuración.

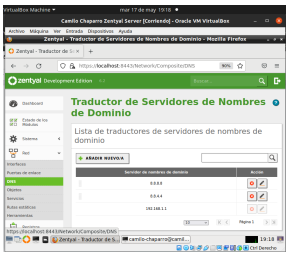

Figura 49. Configuración DNS

A continuación se crean dos objetos, el primero representa la red interna.

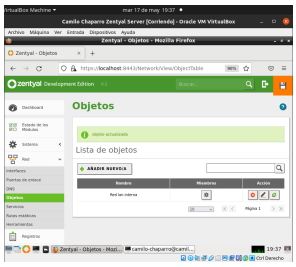

Figura 50. Creación objeto “Red interna”

Una vez creado el objeto, se crea un miembro que pertenece a este (Servicio al cliente), en este paso, seleccionamos el rango de ip que corresponde a la red interna.

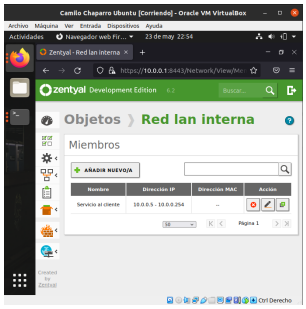

Figura 51. Creación miembro “Servicio al cliente”

Cuando se ha creado el objeto red interna, se crea el objeto que representa los dominios a los cuales los host de la red interna no pueden acceder (sitios de entretenimiento y redes social), para determinar la dirección ip de estos sitios, nos apoyamos en la utilización de los comandos ping o nslookup, junto con el nombre de domino.

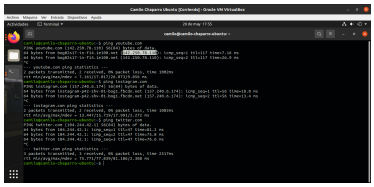

Figura 52. Ejecución comando ping + nombre de dominio

La respuesta de la ejecución de estos comandos son bien la dirección ip (ping), o las direcciones del dominio (nslookup), así que para determinar el CIDR, que se solicita en la creación de los miembros del objeto “sitios web”, nos apoyamos en la página de ARIN (American registry for internet numbers), la cual nos muestra información relacionada a la dirección ip de sitio ingresada.

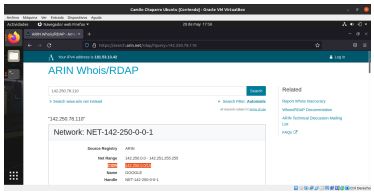

Figura 53. Respuesta consulta ip 142.250.78.110

Una vez tenemos el CIDR de los sitios que se requieren, se crean los miembros del objeto “sitios web”.

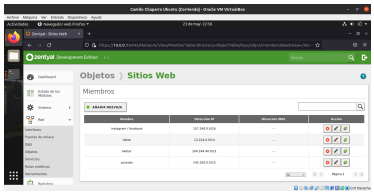

Figura 54. Miembros objeto “sitios web”

Una vez se han creado los objetos de red, Zentyal lista los objetos creados

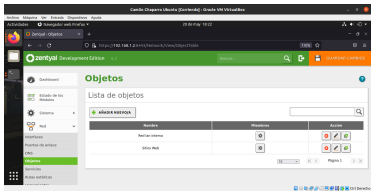

Figura 55. Resumen objetos creados

Una vez han sido creados los objetos de red, se crean las reglas, para ello, se selecciona la opción firewall en el menú a la izquierda, y dentro de este se selecciona la opción filtrado de paquetes.

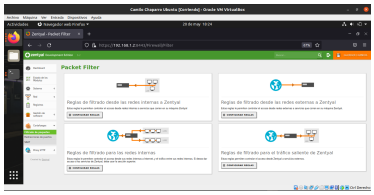

Figura 56. Opción cortafuegos >> Filtrado de paquetes

Al ingresar, se selecciona la opción “reglas de filtrado para las redes internas”, ya que se debe denegar el acceso desde la red interna a internet para las páginas solicitadas.

Figura 57. Opción “Reglas de filtrado para las redes internas”

Al dar clic en configurar reglas, se visualiza la regla que ha sido creada por defecto, la cual permite todos los servicios para todos los orígenes y todos los destinos, esta regla es la que hace posible que los host de la red interna tengan acceso a internet.

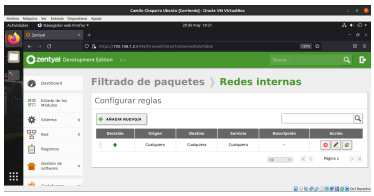

Figura 58. Regla por defecto

Para comprobar que esta regla está funcionando y los host de la red interna tienen acceso a internet, se puede ingresar a cualquier sitio en el navegador de algún host, como por ejemplo youtube, o hacer ping a cualquier dominio.

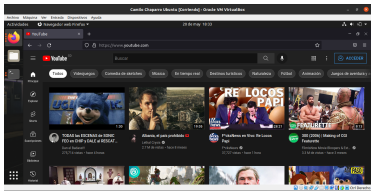

Figura 59. Comprobación ingreso a internet

Una vez se ha comprobado que los host de la red interna tienen acceso a internet, se procede a crear la regla que va a denegar el permiso para que estos host accedan a los recursos solicitados a saber.

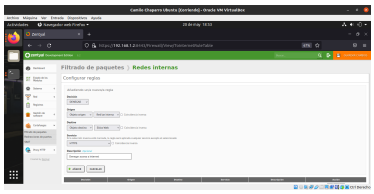

Figura 60. Creación de las reglas

Al darle clic a “añadir”, se puede observar que la regla queda de primera en la lista, lo cual indica que se evaluará primero esta regla, y dependiendo de su resultado se ejecutarán las siguientes en el orden en que se visualizan.

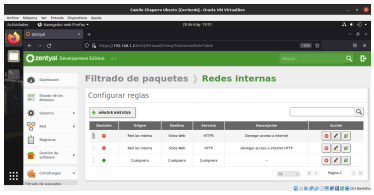

Figura 61. Lista de reglas creadas

Una vez se han creado las reglas, se procede a verificar que ahora no se puede acceder a los sitios solicitados, adicionalmente, se verifican algunos sitios en los que no hay restricciones.

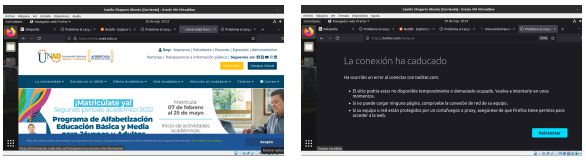

Figura 62. Verificación acceso a sitios web

7 TEMÁTICA 4. FILE SERVER Y PRINT SERVER

Para la configuración del recurso compartir ficheros e impresoras se validará el estado de los módulos. Sí el Controlador de dominio, archivos compartidos y DNS ya se encuentran instalados en el servidor a través de la interfaz de administración.

Figura 63. Ingreso al programa Zentyal.

Sí no están instalados los seleccionamos y continuamos.

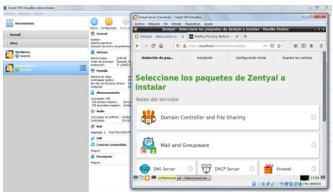

Figura 64. Panel de control para la instalación de paquetes.

Es posible también actualizarlos sí ya se encuentran instalados.

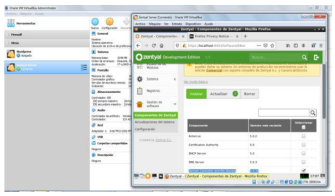

Figura 65. Verificación de componentes de Zentyal

Los servicios como el controlador de dominio permite identificar todos los usuarios, equipos y recursos autorizados a través de los roles de seguridad. El servicio DNS resuelve nombres de equipos en la red asociados a una IP y el módulo de compartir ficheros, para administrar y habilitar carpetas y/o recursos a compartir en la red.

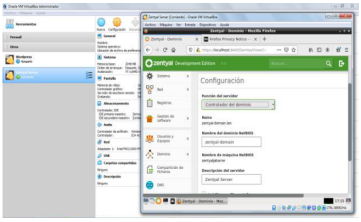

Figura 66. Confirmación de aplicación de cambios.

Ahora validamos los usuarios, grupos y equipos conectados en la red local.

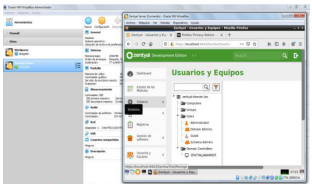

Figura 67.Árbol de equipos

Ingresamos al módulo compartición de ficheros para habilitar un directorio nuevo y/o bajo la raíz y guardamos cambios.

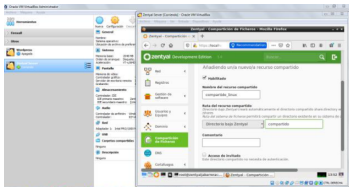

Figura 68. Compartir fichero.

En este módulo se pueden compartir los directorios que considere y a los usuarios que se asignen. También se puede ingresar como invitado al contenido de la carpeta si se habilita la opción. En este caso se crea el fichero compartido linux.

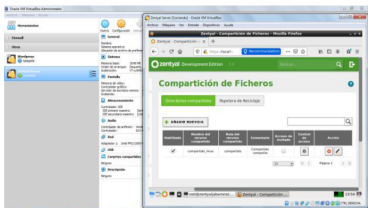

Figura 69. Carpeta compartida en el servidor.

El usuario asignado a esta carpeta se llama empleado, usuario con permisos de lectura y escritura sobre el directorio compartido creado.

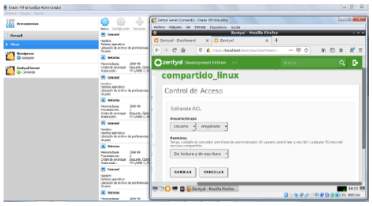

Figura 70. Control de acceso a carpeta compartida.

Asignamos una IP fija al servidor Zentyal y con el comando ifconfig validamos la IP que tiene el equipo.

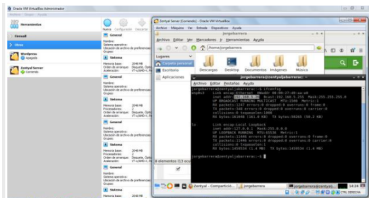

Figura 71. Dirección IP del servidor.

Ahora desde un equipo con Windows 7 en el mismo segmento de red, validamos los sitios de red para encontrar el equipo servidor. También a través del comando ejecutar con la IP podemos acceder al recurso compartido.

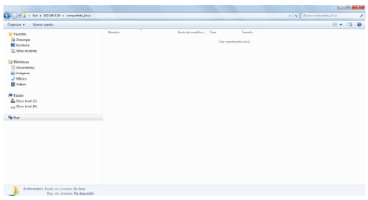

Figura 72. Recurso compartido en la red.

Cuando ingresamos a este directorio fue necesario agregar las credenciales del usuario y contraseña creados en el árbol de usuarios y equipos del servidor Zentyal. Como tiene rol de lectura y escritura desde el sistema operativo de Windows 7 se crea carpeta y archivo en Excel para confirmar la correcta aplicación de seguridad en el directorio.

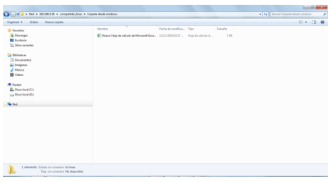

Figura 73. Carpeta creada desde Windows 7.

Para instalar y configurar el servidor de impresoras Zentyal en la red no se realiza directamente desde la interfaz administradora sino desde la interfaz CUPS.
Por defecto el puerto es el 631 y se accede mediante el protocolo HTTPS a través de un navegador habilitado para que escuche.Para la autenticación se usará el mismo usuario y contraseña con el que se accede al servidor. Una vez iniciada sesión añadimos la impresora a través del menú Impresoras, luego añadir Impresora, se debe seleccionar el tipo de impresora y la forma como está conectada a la red, por USB o IP fija. Se debe establecer el fabricante, modelo y controlador, una vez finalizado el asistente, ya tenemos la impresora configurada. Por último dentro del apartado de Control de acceso se puede configurar el control de acceso a los usuarios y grupos creados en el servidor.

8 TEMÁTICA 5. VPN

1.1 Para realizar la instalación de un servidor VPN en Zentyal debemos realizar las siguientes actividades:

En primer lugar, debemos seleccionar qué funcionalidades queremos incluir para nuestro caso, buscaremos la instalación de VPN una vez la ubiquemos la seleccionamos y damos clic en instalar.

Figura 74. Instalación de VPN

Al dar clic en instalar el asistente nos mostrará los paquetes necesarios para la instalación y configuración de VPN, dentro de los que se encuentran configuración de red, firewall, certificado y VPN, damos clic en continuar.

Figura 75. Instalación de paquetes y VPN

Una vez damos clic en instalar el asistente inicia su proceso de instalación una vez termine nos informará que la instalación se realizó correctamente y completa

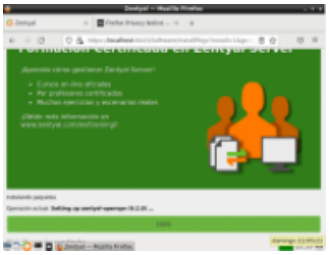

Figura 76. Finalización de la instalación

Debemos validar que la máquina virtual donde tenemos instalada zentyal debe tener dos adaptadores de red habilitados el primero debe estar como adaptador puente y el segundo como red interna.

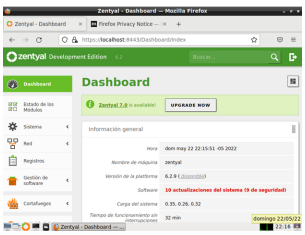

Figura 77. Validación de actualizaciones de Zentyal

Al dar clic sobre actualizaciones nos abrirá una nueva ventana los componentes actualizar, para este caso los seleccionamos todos y damos clic en actualizar

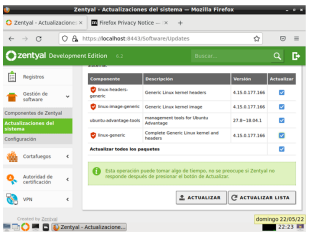

Figura 78. Inicio de Actualización de Zentyal

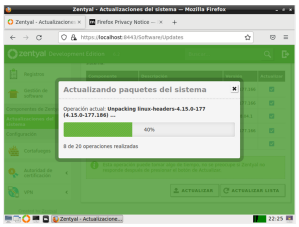

Figura 79. Proceso de instalación actualización Zentyal

Una vez terminada la actualización el asistente nos indicará que se ha completado la instalación con éxito para finalizar damos clic en OK

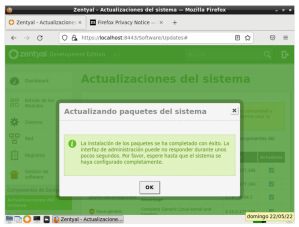

Figura 80. Finalización de la actualización Zentyal

1.2 Para la presente actividad debemos realizar las siguiente

Debemos crear una autoridad de certificado, para ello nos dirigimos a la opción de autoridad de certificación – General y allí creamos el certificados configuración

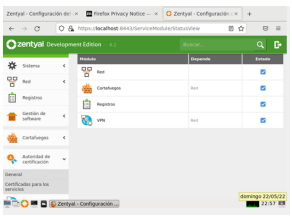

Figura 81. menú de creación de certificados

Una vez ingresada a esta opción el asistente nos pedirá datos de nombre de organización, código de país, ciudad, estado y días para expirar el nombre y los días a expirar son obligatorios los demás campos son opcionales para este caso el nombre que compremos al certificado será CA-Zentyal

Figura 82. Configuración de certificado para servidor VPN

Una vez creado el certificado lo podemos ver en la parte inferior de la pantalla dentro de la lista de certificado actuales

Figura 83. Lista de certificados actuales para server VPN

Ahora guardamos los cambios dando clic en el boto de guardado y confirmamos que se desean guardar los cambios realizados

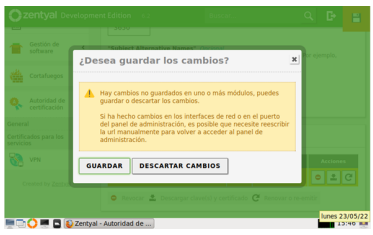

Figura 84. Confirmación para guardar cambios

Una vez finalizado el proceso el sistema nos indicará que se ha guardado correctamente los cambios

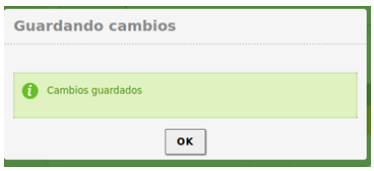

Figura 85. Cambios guardados

Una vez se tengan el certificado, procedemos a la creación del servidor VPN en Zentyal para ello nos vamos a la opción de VPN – Servidores y damos clic en añadir nuevo

Figura 86. Opción para añadir nuevo servidor VPN

El único dato que necesitamos para crear el servidor VPN es el nombre en este caso le pondremos ladyserver.vpn

Figura 87. Configuración de nombre para servidor VPN

Ahora guardamos los cambios dando clic en el botón de guardado y confirmamos que se desean guardar los cambios realizados

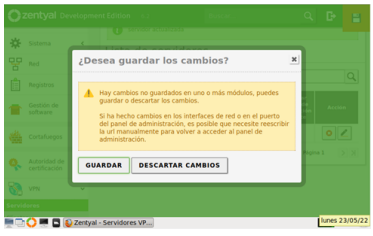

Figura 88. Confirmación para guardar cambios

Una vez finalizado el proceso el sistema nos indicará que se ha guardado correctamente los cambios

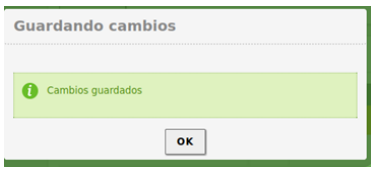

Figura 89. Cambios guardados

Ya finalizada la creación del servidor de VPN, nos dirigimos nuevamente a la opción de autoridad de certificados – General donde debemos crear un nuevo certificado para el servidor ya que el anterior correspondía para el servidor VPN, ingresamos nombre común y días de expiración

Figura 90. Creación de certificado Server

Una vez creado el certificado para el server nos ubicamos en la parte inferior de la pantalla y podemos ver los 2 certificados creados

Figura 91. Lista de certificados creados

Una vez creado los dos certificados y el servidor VPN nos dirigimos nuevamente a la opción de VPN-Servidores y damos clic en configuración

Figura 92. Opción de configuraciones de servidor VPN

Dentro de la configuración podremos ver las configuraciones realizadas por defecto, si se desea se puede modificar, en mi caso dejaremos lo único que se

hará es habilitar la opción de interfaz tun y damos clic en cambiar

Figura 93. Configuración VPN parte 1

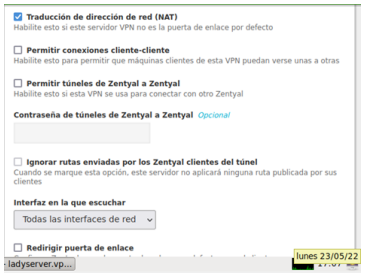

Figura 94. Configuración de VPN parte 2

Ahora guardamos los cambios realizados en la configuración anterior dando clic en el botón de guardar

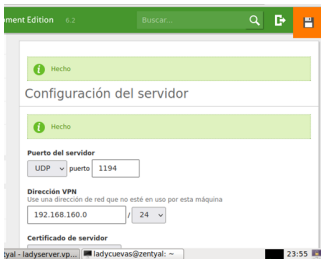

Figura 95. Guardar cambios

Una vez creado y configurado el servidor VPN debemos realizar la configuración de comunicación con el servidor para ello haremos dos configuraciones la primera será en los servicios y la segunda en el cortafuegos todo esto para que permita la comunicación mediante los puertos configurados en el servidor VPN

A .Para configurar los servicios nos vamos al menú de Zentyal y damos clic en la opción Red – Servicios y damos clic en añadir nuevo servicio.

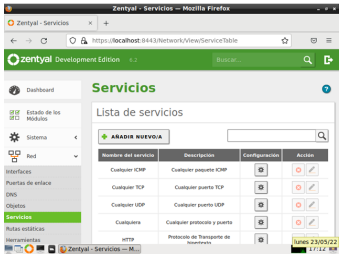

Figura 96. Configuración de servicios

Para crear el nuevo servicio solo necesitamos colocar un nombre de servicio en este caso colocaremos RedVPN y descripción Servicio de red VPN luego damos clic en añadir

Figura 97. Creación de servicios RedVPN

Ahora procedemos a configurar el servicio que acabamos de crear para lo cual nos ubicamos en la lista de servicios y damos clic en el botón de configurar

Figura 98. Pestaña de configuración de servicios

Debido a que el servicio es nuevo debemos añadir nueva configuración para ello damos clic en la opción de añadir nuevo

Figura 99. Pestaña para agregar nueva configuración del servicio

Ahora debemos configurar el servicio en el cual debemos indicar el protocolo que definimos en la

configuración del servidor VPN que es protocolo UDP, en la opción de puerto de origen vamos a colocar cualquiera y en el puerto de destino seleccionamos puerto único que va ser 1194, esto lo que está haciendo es permitiendo que se pueda ingresar desde cualquier red a el puerto designado en destino

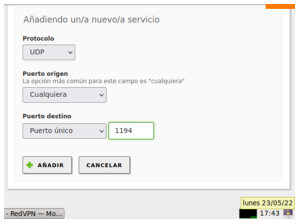

Figura 100. configuración del servicio red VPN

Una vez añadida la configuración procedemos a guardar los cambios con el botón guardar el asistente nos preguntará si deseamos guardar los cambios damos clic en guardar

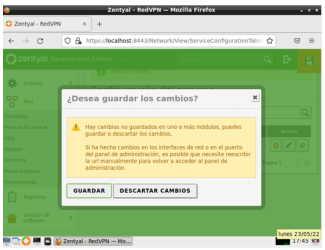

Figura 101. Guardar cambios realizados

Una vez guardado los cambios podremos ver como quedó configurado el servicio

Figura 102. Detalle de configuración de servicio

Ahora realizaremos la configuración del cortafuegos desde Zentyal para ello nos vamos al menú a la opción de cortafuegos – Filtrado de paquetes – reglas de filtrado desde las redes interna a Zentyal y damos clic en configurar reglas

Figura 103. Pestaña de configuración de reglas cortafuegos

Dentro de la configuración de las reglas de cortafuego, procedemos agregar una nueva regla con el servicio creado anteriormente, para ello damos clic en añadir nuevo

Figura 104. Pestaña para añadir nueva regla

Para crear la nueva regla debemos seleccionar las acciones a realizar en la opción de decisión colocamos aceptar en el origen seleccionamos cualquiera, en servicio el que creamos anteriormente RedVPN y una descripción, para finalizar damos clic en añadir, con esta regla lo que estamos haciendo en permitir la conexión desde cualquier origen al destino configurado en el servicio que es el puerto UDP 1194

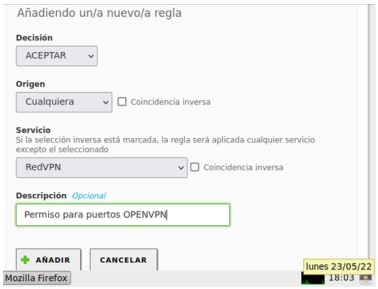

Figura 105. Configuración de regla de firewall

Procedemos a guardar los cambios dando clic en el botón guardar y confirmando que deseamos guardar los cambios realizados

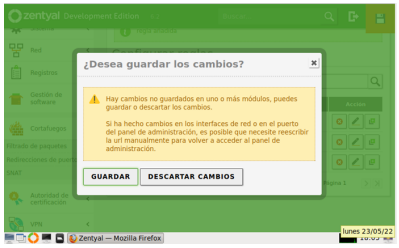

Figura 106. Guardar cambios regla firewall

Procedemos a realizar la descarga del paquete de la configuración del cliente para ello nos vamos a la opción VPN – Servidores- descarga de paquete de instalación de cliente y damos clic en configuración

Figura 107. Pestaña de servidor VPN

Una vez en la configuración del paquete de descarga ingresamos el tipo de cliente donde vamos a instalar la VPN, en nuestro caso Windows, el certificado del cliente para este caso anteriormente habíamos creado el certificado cliente.lady chequeamos la opción de instalar openVPN para Windows, en la dirección del servidor colocamos la ip publica de internet en nuestro caso 190.25.29.68, y en la dirección adicional del servidor la ip de la WAN de zentyal 192.168.0.79, una vez ingresado estos datos damos clic en descargar

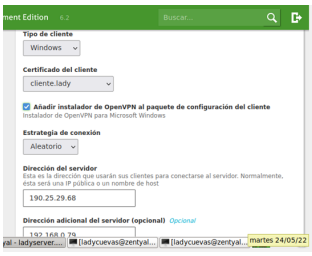

Figura 108. Configuración y descarga de cliente VPN

Una vez descargada la configuración la trasladamos al equipo cliente en este caso será mi equipo físico el cual no se encuentra en la red interna de Zentyal, esto lo haremos mediante la herramienta de Drive de Google

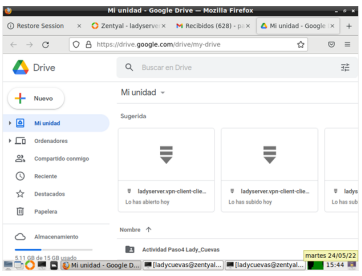

Figura 109. Carpeta de Google Drive

Ya descargado el paquete en el equipo cliente realizamos la descompresión del archivo comprimido y ejecutamos el instalador de openVPN de Windows realizamos la respectiva instalación con la ayuda del asistente dado clic a cada una de las opciones de siguiente y de instalación al finalizar podremos ver el acceso directo de OPENVPN

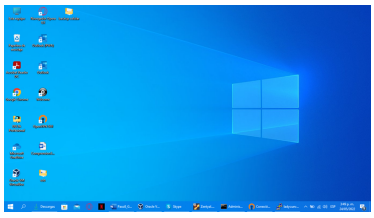

Figura 110. Equipo Windows con OPENVPN

Ya instalado openVPN tomamos los cuatro archivos de certificados que se encuentran en el paquete de descarga que hicimos anteriormente

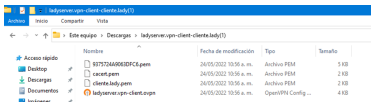

Figura 111. Carpeta de archivos certificado OPENVPN

Los copiamos y los pegamos en la siguiente ruta C:\Users\lady\OpenVPN\config

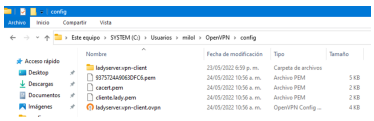

Figura 112. Carpeta destino de archivos certificado OPENVPN

Después de esto procedemos a ejecutar OPENVPN como administrador, automáticamente nos mostrará un icono en la parte inferior de la pantalla al cual debemos dar clic derecho importar archivo y buscamos la ruta donde se encuentra la configuración de vpn en mi caso Los copiamos y los pegamos en la siguiente ruta C:\Users\lady\OpenVPN\config y damos clic en abrir

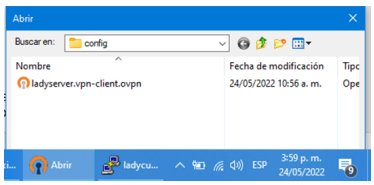

Figura 113. Importación archivo configuración VPN

Ahora procedemos a realizar la conexión para ello nos ubicamos nuevamente en la parte inferior de la pantalla damos clic derecho al icono de OPENVPN y damos clic en conectar

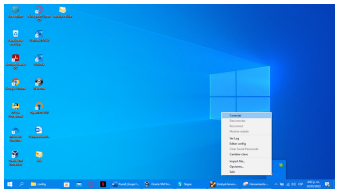

Figura 114. Pestaña para conectar VPN

Al dar clic a la opción de conectar openvpn realiza el proceso de conexión y una vez finalice nos indicará que está conectado y nos mostrara la ip designada

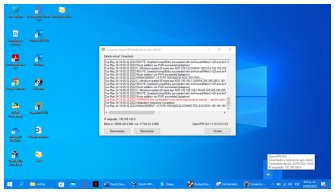

Figura 115. Conexión VPN

Para validar que la conexión se realizó correctamente y que está funcionando realizaremos varias pruebas

1.Validamos que en equipo cliente Windows no esté configurada la ip interna de zentyal 192.168.1.0/24, que exista la conexión por túnel con un segmento de red 192.168.160/24

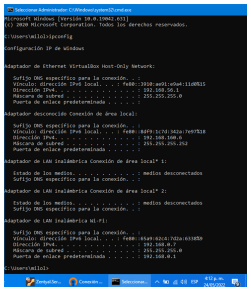

Figura 116. Validación configuración red equipo cliente Windows

2. Validamos que funcione el ping hacia la ip interna de zentyal 192.168.1.1

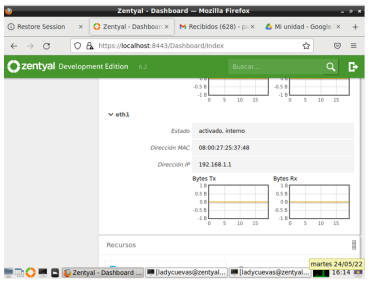

Figura 117. IP Interna de Zentyal

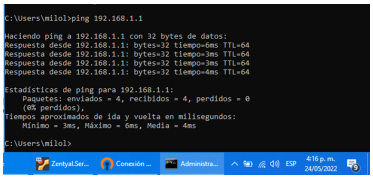

Figura 118. Ping a IP Interna de Zentyal

3. Ingresamos al dashboard de zentyal y verificamos las conexiones establecidas actualmente mediante la VPN y podemos validar la del cliente Windows

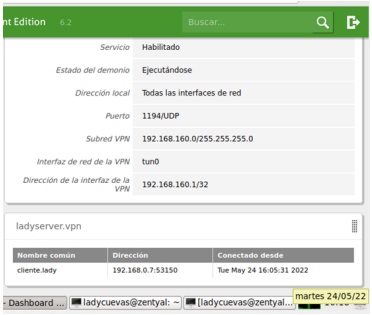

Figura 119. Ping a IP Interna de Zentyal

4. Realizamos una conexión por ssh a zentyal utilizando la aplicación de Putty desde el equipo cliente de Windows.

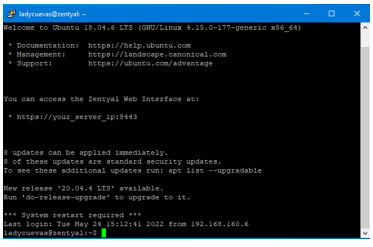

Figura 120. Conexión ssh Zentyal

9 CONCLUSIONES

Zentyal es una alternativa viable para reemplazar sistemas de "administración Windows", la administración de Zentyal es fácil e intuitiva siempre y cuando se tengan conocimientos sobre infraestructura informática, no tiene funcionalidades avanzadas nativas para la configuración de GPO, No es competencia para alternativas en nube como Azure AD, o intune ya que se limita a directorio activo de forma local

Un Proxy es un equipo informático que hace de intermediario entre las conexiones de un cliente y un servidor de destino, filtrando todos los paquetes entre ambos. Las ventajas que tiene es que posee un máximo control sobre las conexiones y una elevada monitorización y registro. Dentro de sus inconvenientes está la pérdida de rendimiento. La diferencia que hay entre Proxy y VPN es que el primero simplemente dirige el tráfico hacia su destino y el segundo cifra todo el tráfico entre el dispositivo y el servidor VPN.

El firewall es una herramienta que ayuda a incrementar la seguridad de la red ya que permite gestionar y controlar el tráfico en una red interna así como filtrar los paquetes que llegan a la red desde el exterior y crear reglas para conceder o denegar servicios específicos según protocolos, lo que brinda un mejor control sobre el tráfico de red desde y hacia la red administrada.

Se puede concluir que Zentyal Server es una alternativa viable para implementar un sistema de File Server ya que es compatible con sistemas Windows a través de SMB y protocolos de autenticación de usuario, esto unido a su rol de Directorio activo garantiza una muy completa plataforma de centralización y administración de permisos en activos de información almacenados en carpetas, la administración de cola de impresión centralizada garantiza un uso óptimo del recurso y la posibilidad de controlar de maneras eficientes las cargas de trabajo enviadas a este.

El servidor VPN permite que las empresas puedan acceder desde redes externas a sus equipos y servidores de una manera confiable y segura. Hoy en día la mayoría de las compañías requieren este tipo de conexiones debido a la nueva modalidad de trabajo conexión remota a causa de la contingencia vivida por el COVID 19, esta herramienta se puede adquirir a un bajo costos a comparación con una herramienta no libre, su interfaz es muy amigable y puede ser instalado bajo sistemas operativos Windows y Linux, según la necesidad de cada cliente.

10 REFERENCIAS

[1] Unir clientes Ubuntu y Windows a Zentyal. YouTube: https://www.youtube.com/watch?v=hQn4tvIaHJc&t=181s

[2] Releases · BeyondTrust/pbis-open · GitHub: https://github.com/BeyondTrust/pbis-open/releases

[3] Zentyal 7.0 Documentación Oficial — Documentación de Zentyal 7.0: https://doc.zentyal.org/es/

[4] Avast academy. Recuperado en marzo de 2020. https://www.avast.com/es-es/c-what-is-a-proxy-server.

[5] Jose Giménez.(2014, Seguridad en equipos informaticos. https://books.google.com.co/books?id=N1YpEAAAQBAJ&pg=PT424&dq=proxy+que+es&hl=es&sa=X&ved=2ahUKEwi54ePPvIz4AhXynHIEHZ9jAnYQ6AF6BAgJEAI#v=onepage&q=proxy%20que%20es&f=false.

[6] American Registry for internet numbers ARIN Whois/RDAP. https://search.arin.net/rdap/?query=142.250.78.110

[7] IBM. Direccionamiento interdominio sin clase. recuperado en mayo de 2022. https://www.ibm.com/docs/es/i/7.2?topic=methods-classless-inter-domain-routing

[8]Oracle. Glosario de términos de redes. recuperado junio 2022. https://docs.oracle.com/cd/E56339_01/html/E53820/gnchw.html

[9] Zentyal Community, Documentación de zentyal, recuperado mayo de 2022. https://doc.zentyal.org/6.2/es/

[10] Qué es un Print Server, tomado de Wikipedia,https://es.wikipedia.org/wiki/Sistema_de_nombres_de_dominio

[11] Servicio de resolución de nombres de dominio (DNS) - Zentyal Linux Small Business Server. (2019). Tomado de de https://wiki.zentyal.org/wiki/Es/4.1/Servicio_de_resolucion_de_nombres_de_dominio_(DNS)

[12] Ramírez, I. (2021, 29 enero). ¿Qué es una conexión VPN, para qué sirve y qué ventajas tiene? Xataka. https://www.xataka.com/basics/que-es-una-conexion-vpn-para-que-sirve-y-que-ventajas-tiene

[13] N. (s. f.). Seguridad de la información electrónica. El Certificado Digital. Digitalizing be people. https://blog.neteris.com/stepforward/seguridad-de-la-informacion-electronica.-el-certificado-digital#:%7E:text=Un%20certificado%20digital%20es%20un,su%20identidad%20digital%20en%20Internet.

[14] Servicio de redes privadas virtuales (VPN) con OpenVPN — Documentación de Zentyal 6.2. (s. f.). Zentyal Comunity. https://doc.zentyal.org/6.2/es/vpn.html