

INSTALACIÓN Y CONFIGURACIÓN DE ZENTYAL SERVER EN LA GESTIÓN DE INFRAESTRUCTURA IT

Darío Segundo López
dslopezr@unadvirtual.edu.co
Diana Marcela Enríquez
dmenriquezl@unadvirtual.edu.co
Diego Alejandro Gutiérrez
dgutierrezl@unadvirtual.edu.co
Felipe García Londoño
fgarcialo@unadvirtual.edu.co
Miguel Ángel Herrera Echeverry
maherrerae@unadvirtual.edu.co

Universidad Nacional Abierta y a Distancia UNAD, Escuela de Ciencias Básicas, Tecnología e Ingeniería, Colombia - Mayo de 2021

RESUMEN: A lo largo de los diferentes módulos del diplomado de profundización en Linux, se ha podido evidenciar la posibilidad de soluciones robustas y estables a través de servidores en base a tecnología Linux para las empresas, Zentyal ofrece servicios confiables y funcionales que están a la vanguardia de las tecnologías y necesidades actuales. El presente documento describe el paso a paso de la instalación de Zentyal Server, su configuración inicial, así como la implementación de los siguientes servicios: DHCP Server, Proxy no transparente, Cortafuegos, File Server y Print Server, y VPN verificando su funcionamiento tanto en el servidor como en el equipo cliente asociado.

ABSTRACT: Throughout the different modules of the Specialization course in Linux, it has been possible to demonstrate the possibility of robust and stable solutions through servers based on Linux technology for companies, Zentyal offers reliable and functional services that are at the forefront of current technologies and needs. This document describes the step-by-step installation of Zentyal Server, its initial configuration, as well as the implementation of the following services: DHCP Server, Non-transparent Proxy, Firewall, File Server and Print Server, and VPN, verifying its operation both in the server as well as the associated client computers.

PALABRAS CLAVE: Controlador de Dominio, Cortafuegos, File Server, VPN, Zentyal

1 INTRODUCCIÓN

En el transcurso del diplomado se ha configurado e implementado diferentes servicios en servidores Linux, ya sea por terminal o entorno gráfico. En el presente informe se expone una solución al requerimiento planteado para el paso 8 que recopila la aplicación del aprendizaje obtenido en las unidades del diplomado de Linux como opción de grado, entregando el proceso de

cada una de las actividades y documentando su desarrollo, en este registro se ve el paso a paso de la instalación del servidor Zentyal server, un servidor muy interesante, versátil y con una interfaz bastante intuitiva, se realiza la configuración inicial de funcionamiento y la instalación de todos los módulos y servicios, probando el funcionamiento de los servicios mediante la conexión de un equipo cliente.

2 INSTALACIÓN DE ZENTYAL SERVER

Se inicia el instalador de Zentyal y se selecciona la segunda Opción, "Expert Mode"

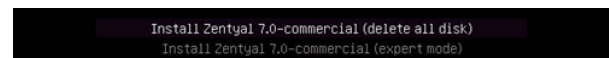


Imagen 1. Expert Mode.

Posteriormente entre los idiomas de instalación se selecciona "Español".



Imagen 2. Selección del idioma.

Se selecciona el país, para este caso Colombia.

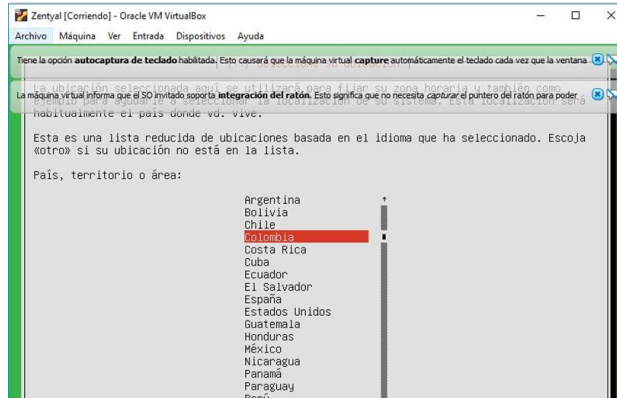


Imagen 3. Selección del país.

Se indica que si, a la opción de identificar la distribución del teclado.

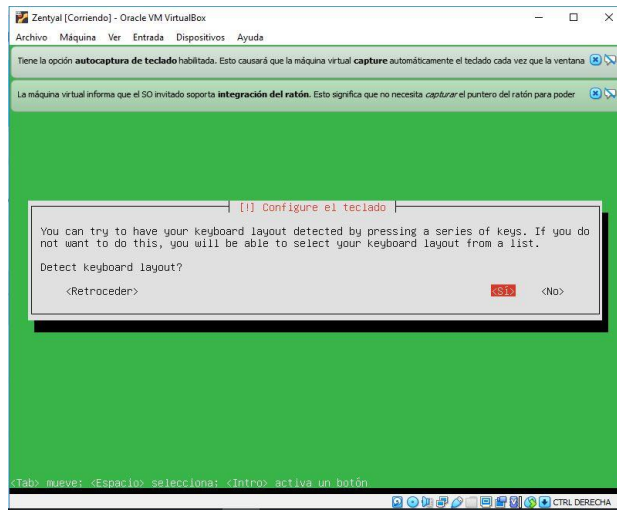


Imagen 4. Distribución de teclado

Se presionan algunas teclas para el reconocimiento de estas.

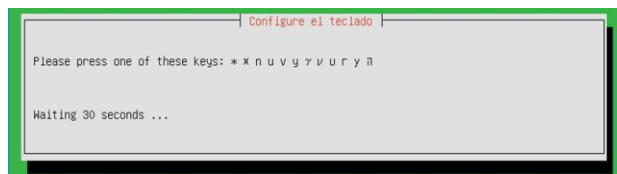


Imagen 5. Presionar Teclas

Finalmente se reconoce la distribución de teclado y se continua el proceso.

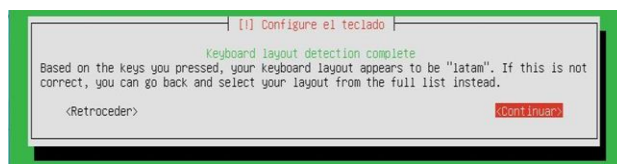


Imagen 6. Continuar

Continúa la instalación con la descarga de algunos complementos.

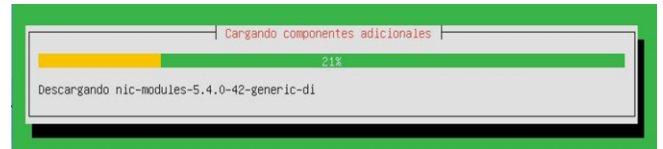


Imagen 7 Instalando complementos

Se establece el nombre del servidor:

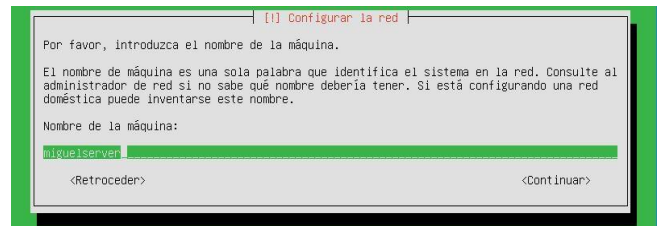


Imagen 8. Hostname

Se ingresa el nombre de usuario

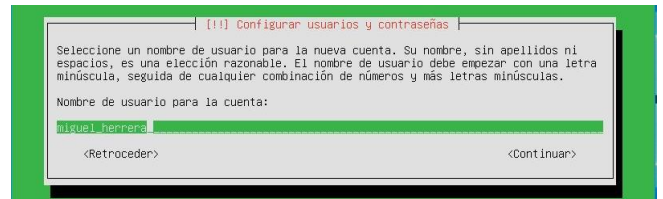


Imagen 9. Usuario

Se asigna la contraseña al usuario.

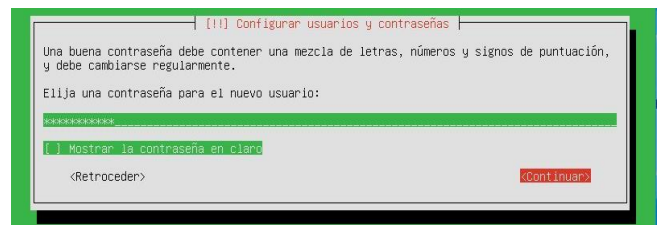


Imagen 10. Contraseña

Se confirma la zona horaria identificada.

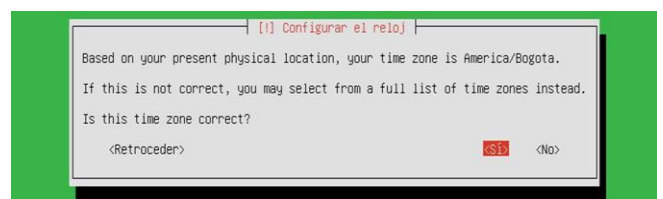


Imagen 11. Zona Horaria

Se selecciona la opción de utilizar todo el disco.

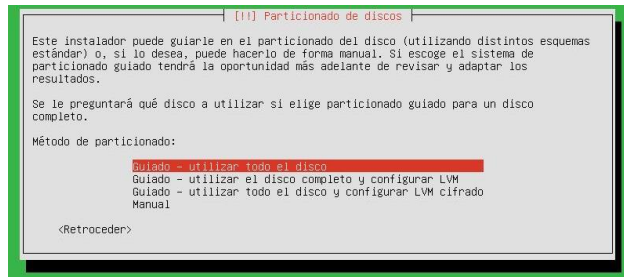


Imagen 12. Todo el disco

Se elige el disco para la instalación.

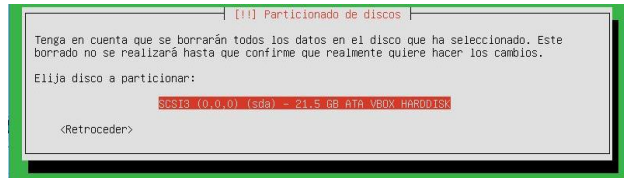


Imagen 13. Disco para instalación

El instalador indica cómo van a ser creadas las particiones en el disco y se confirma que sí.

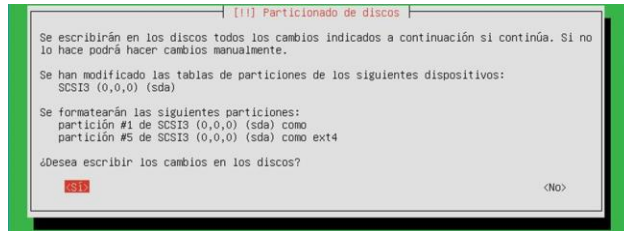


Imagen 14. Particiones

Se selecciona la opción de no para la instalación con entorno gráfico.

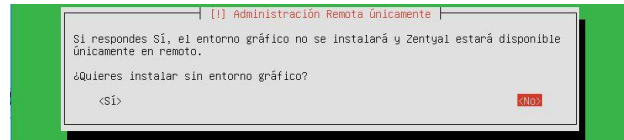


Imagen 15. Modo gráfico

No se utiliza proxy así que se da clic en continuar.



Imagen 16. Proxy

Se empieza a descargar e instalar componentes.

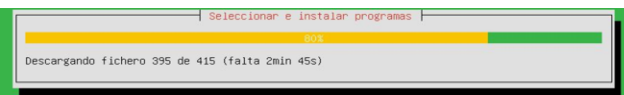


Imagen 17. Descarga Archivos

Se instala el cargador de arranque GRUB en el disco duro.

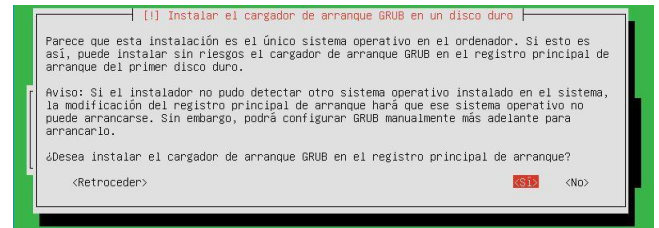


Imagen 18. GRUB

Se establece la hora del reloj en UTC.

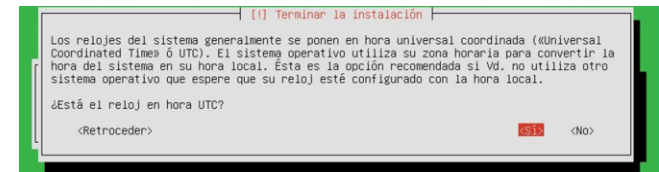


Imagen 19. Reloj UTC

El instalador indica que se ha completado la instalación y se procede a iniciar el sistema.



Imagen 20. Reloj

Con esto el sistema termina de instalar Zentyal.



Imagen 21 Terminar instalación

Zentyal instalado y se inicia en modo desktop



Imagen 22 Zentyal

Al iniciar Zentyal automáticamente se abre el navegador mostrando la dirección local para administrar el servidor Zentyal, <https://localhost:8443>, en la advertencia de riesgo y se da clic en Advanced...

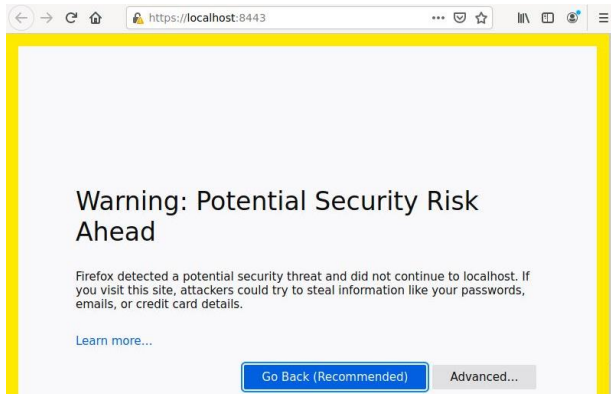


Imagen 23. Localhost

Se da clic en "Accept the Risk and Continue".

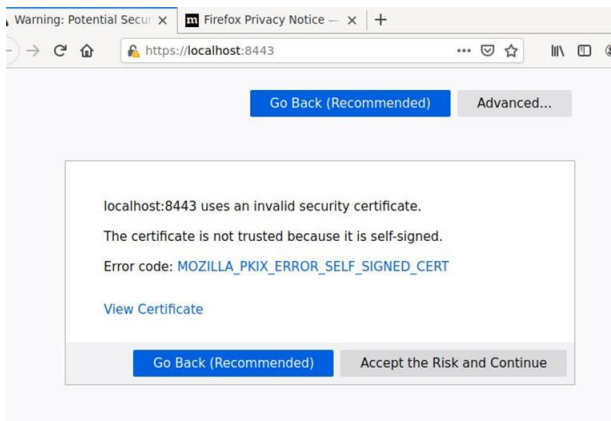


Imagen 24. Aceptar el riesgo

Se ingresa el usuario y contraseña generados en el proceso de instalación.

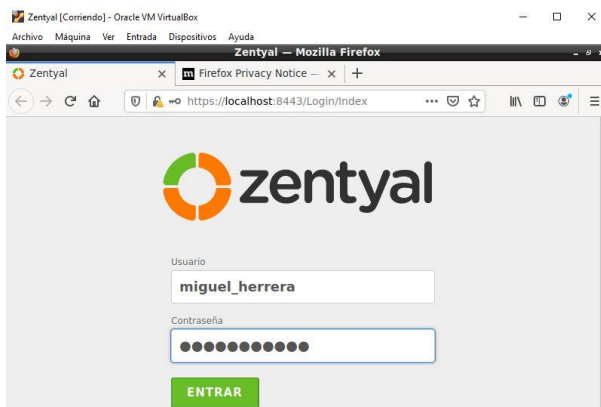


Imagen 25. Inicio Zentyal

Para activar las funcionalidades de Zentyal se ingresa la licencia recibida en el correo y se da clic en el botón "Validar Licencia".



Imagen 26. Activación

3 CONFIGURACIÓN INICIAL ZENTYAL

Se debe realizar las configuraciones iniciales a Zentyal para poner en funcionamiento sus servicios con otros clientes a través de la red del servidor.



Imagen 27. Configuración inicial

En el Dashboard (Panel de control de Zentyal) se encuentra la versión del Zentyal server y a disposición la instalación y configuración de los componentes del servidor.

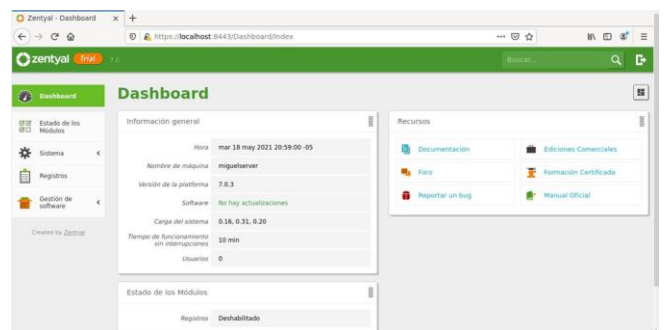


Imagen 28. Dashboard

Inicialmente se da un nombre a la máquina y se deja el dominio por defecto que ya trae escrito.

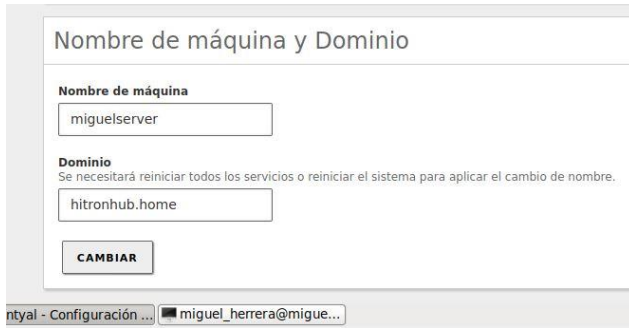


Imagen 29. Hostname

Inicialmente se verifica las interfaces de red, se activa el adaptador de red con el comando dhclient para que tome una IP de red y se pueda tener internet, se verifica la IP entregada con el comando ifconfig.

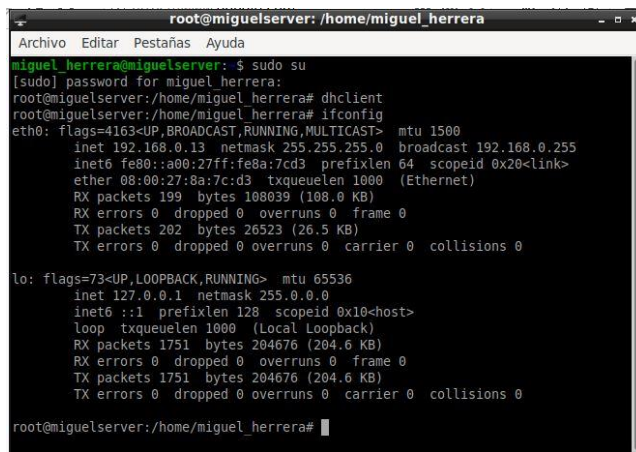


Imagen30. IP de internet

Se actualiza la disponibilidad de repositorios a instalar con los comandos:

apt-get update:

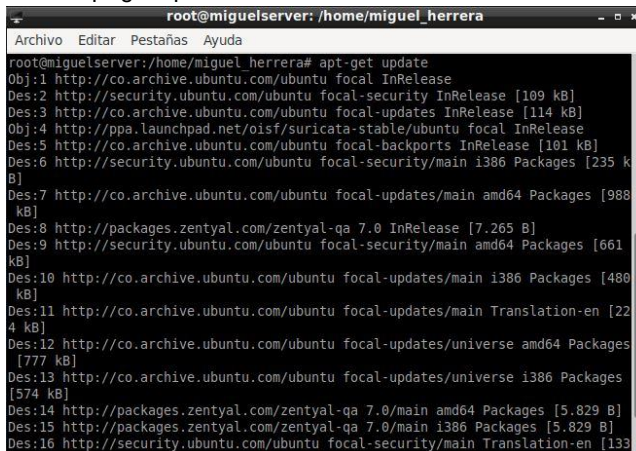


Imagen 31. Apt-get update

Apt-get upgrade

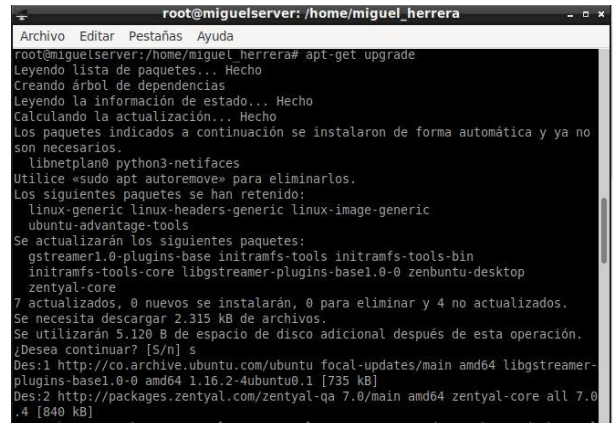


Imagen 32. Apt-get upgrade

Posteriormente se ingresa a la opción Gestión de software y a la pestaña Componentes de Zentyal, allí se selecciona los componentes necesarios, para este caso se instalan Domain Controller and file Sharing, DNS Server, DHCP server, Firewall y se da clic en el botón "Instalar".

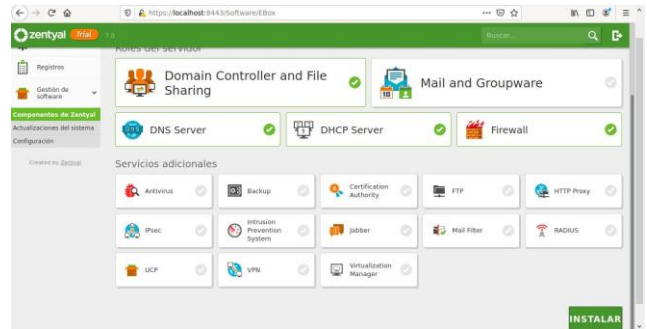


Imagen 33. Instalar componentes

Se muestran los paquetes seleccionados para instalar y se da clic en Continuar.



Imagen 34. Confirmar Instalar componentes

Se empiezan a instalar los paquetes seleccionados en el servidor.



Imagen 35. Instalando paquetes

Se finaliza la instalación de los paquetes.

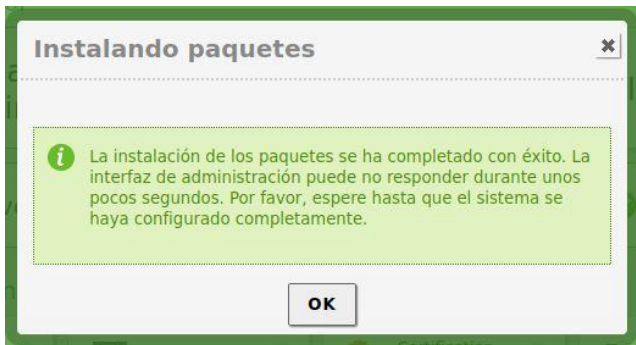


Imagen 36. Paquetes instalados

En la pestaña de Estado de los módulos se activan los módulos instalados.



Imagen37. Estado de módulos

En la pestaña de componentes de Zentyal se verifica los componentes instalados y si se debe actualizar alguno de ellos.

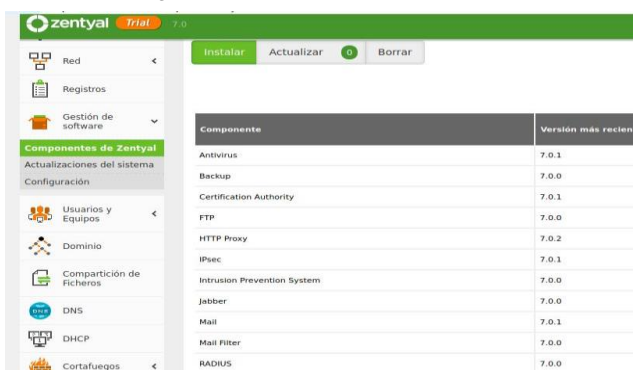


Imagen 38. Componentes Zentyal

Después se configura la red en el servidor, con 2 tarjetas de red, una para la WAN y otra para la LAN, la tarjeta principal de red se establece en modo puente.

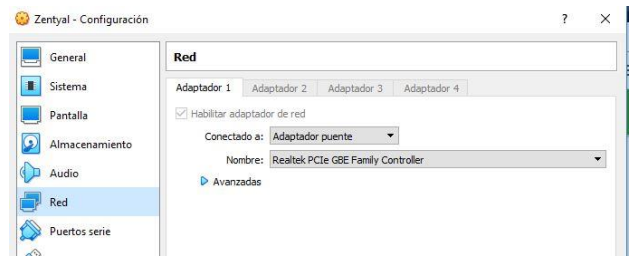


Imagen39. Tarjeta Puente

La tarjeta de red secundaria en modo de Red interna.

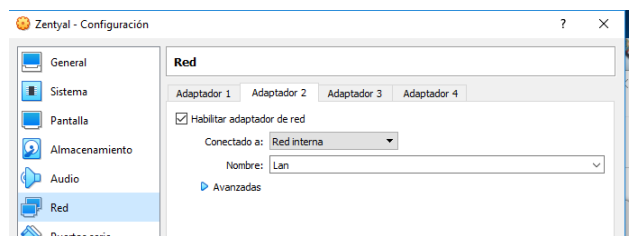


Imagen 40. Red Interna

En el servidor Zentyal, en el módulo de Red – Interfaces, se configura de la siguiente manera:

La red eth0 para la WAN, se establece en el Método DHCP y se activa la casilla Externo (WAN).



Imagen 41. eth0

En la interfaz eth1 se establece el modo Estático, se asigna una dirección IP y máscara de red.



Imagen 42. eth1

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

Se instalan y se activan los paquetes necesarios para la ejecución de los servicios de DNS, DHCP y controlador de dominio.

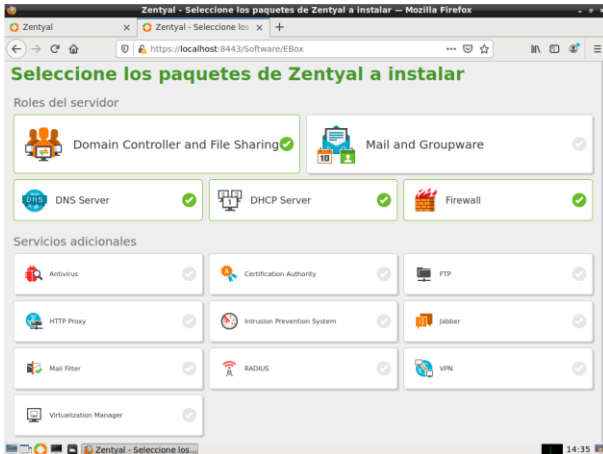


Imagen 43. Instalación paquetes Zentyal

En la configuración de red se asigna el direccionamiento por DHCP a eth0 y direccionamiento estático para eth1 192.168.20.100/24.

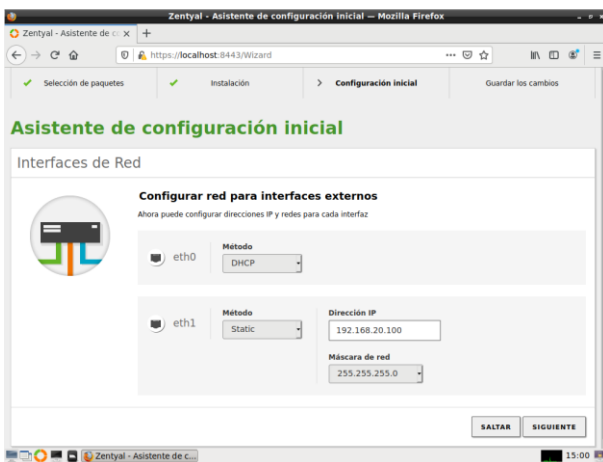


Imagen 44. Asistente de red.

Para dar inicio a la configuración del servidor DNS es necesario establecer el nombre del dominio.

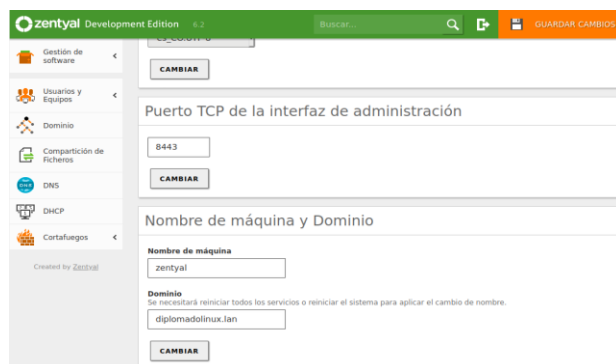


Imagen 45. Nombre de máquina y dominio.

Se procede a la configuración del DNS y se agregan los redireccionadores 8.8.8.8 y 1.1.1.1 para resolver DNS externos se asigna la dirección IP 192.168.20.100 al dominio diplomadolinux.lan y se registra el nombre de la maquina zentyal.

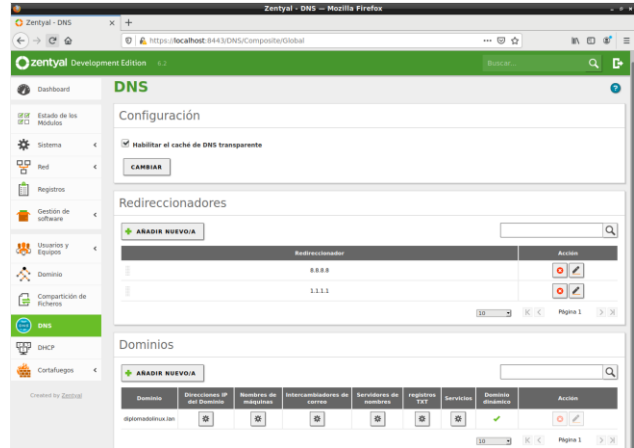


Imagen 46. Instalación de paquetes Zentyal.

Se inicia el proceso de configuración de DHCP en la interfaz eth1, se establece la puerta de enlace predeterminada como Zentyal, el dominio de búsqueda en diplomadolinux.lan y el servidor de nombres primario como DNS local de Zentyal.

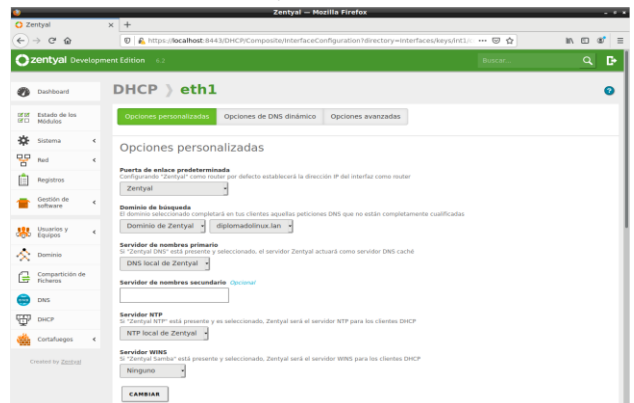


Imagen 47. Configuración DHCP.

Para la asignación de direcciones IP, se establece el rango desde la IP 192.168.168.20.101 hasta la dirección 192.168.20.30

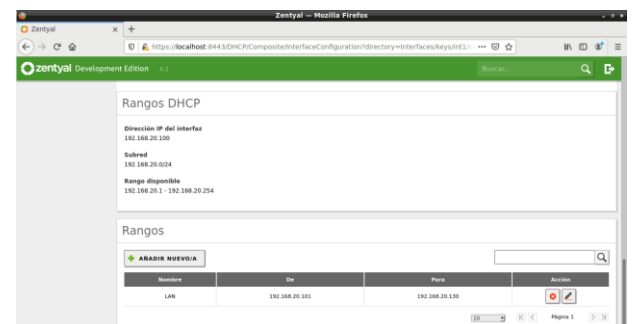


Imagen 48. Rangos DHCP.

Se realiza la prueba de asignación de dirección IP a través de DHCP en un cliente Linux (Ubuntu).

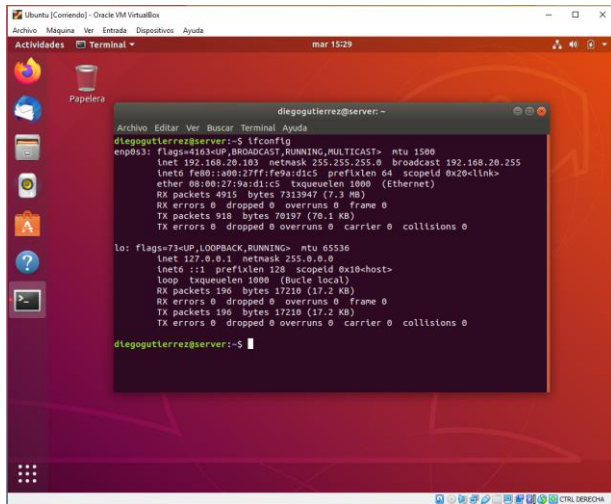


Imagen 49. Comando ifconfig.

Se verifica la resolución de nombres a través de un cliente Linux (Ubuntu).



Imagen 50. Comando nslookup.

En la configuración del controlador de dominio se establece el nombre de dominio de Netbios a diplomadolinux y nombre de maquina zentyl.

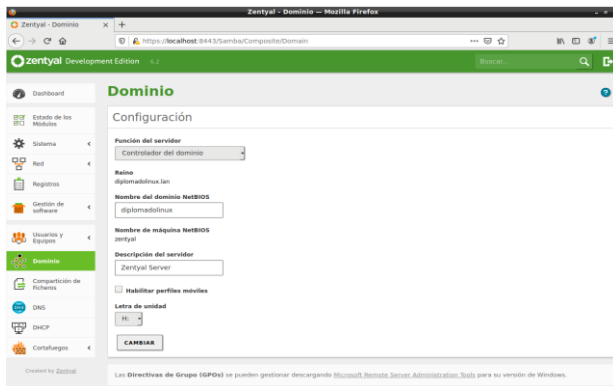


Imagen 51. Configuración dominio.

Se verifica la creación del dominio diplomadolinux.lan

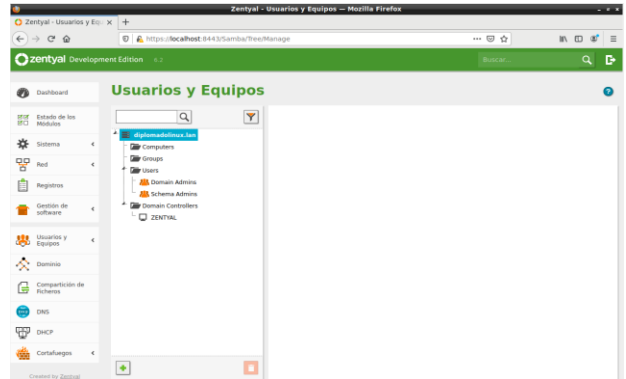


Imagen 52. Usuarios y equipos.

Se crea una nueva unidad organizativa para un mejor control de los usuarios y grupos.

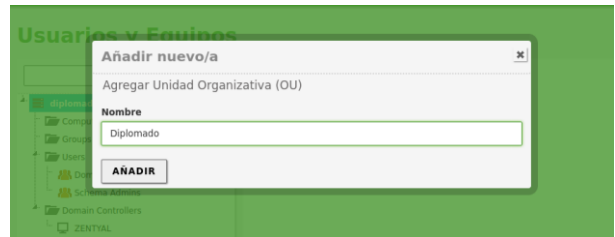


Imagen 53. Agregar unidad organizativa.

Se crea el grupo estudiantes para el control de los usuarios.

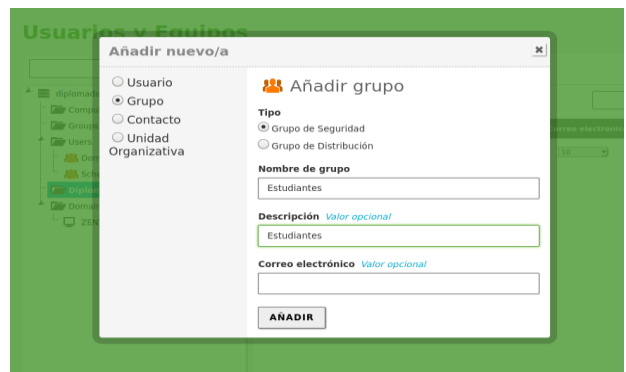


Imagen 54. Añadir grupo.

Se establece la información y contraseña para el usuario administrador.

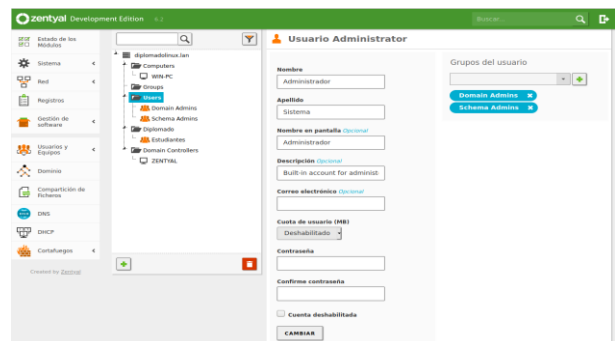


Imagen 55. Actualizar usuario administrador.

Se crean los nuevos usuarios en el grupo de estudiantes.

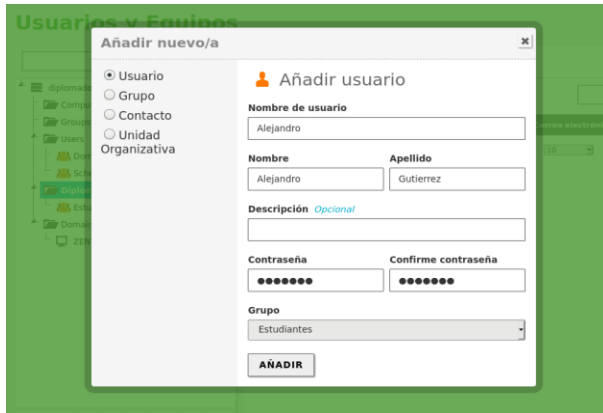


Imagen 56. Añadir usuario.

En el módulo usuarios y grupos se verifica el estado de los nuevos usuarios.

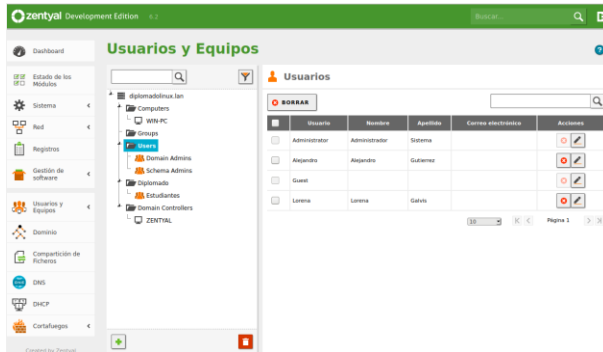


Imagen 57. Usuarios y equipos.

Con los usuarios configurados y activos se procede a configurar la compartición de ficheros, asignando un recurso compartido para cada usuario y el recurso cursos para todos los usuarios.



Imagen 58. Compartición de ficheros.

Se establece la regla para el control de acceso.

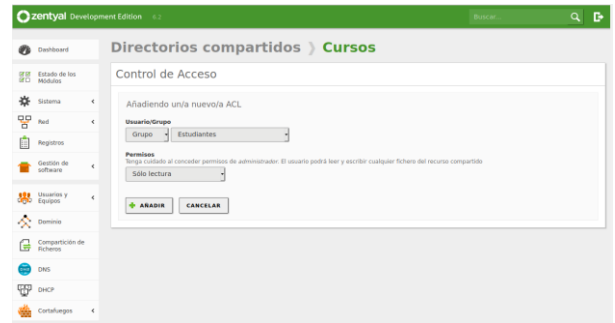


Imagen 59. Control de acceso.

Se verifica el listado de recursos compartidos.

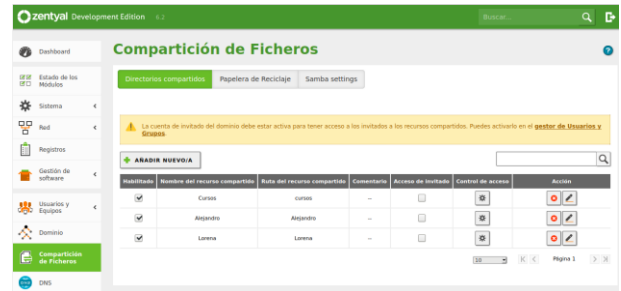


Imagen 60. Instalación paquetes Zentyal.

Se realiza la prueba de conexión mediante el controlador de dominio en un cliente Windows 10.

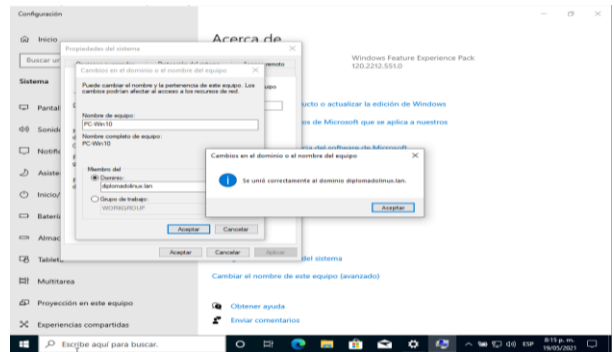


Imagen 61. Agregar miembro al dominio.

Se verifica el inicio de sesión por parte del usuario en el dominio.

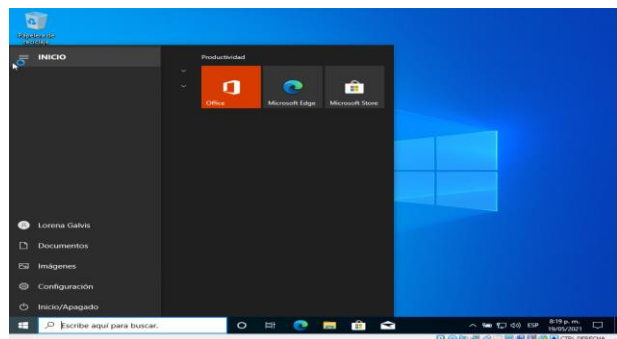


Imagen 62. Inicio de sesión en dominio.

Se visualiza los recursos compartidos en zentyal.diplomadolinux.lan

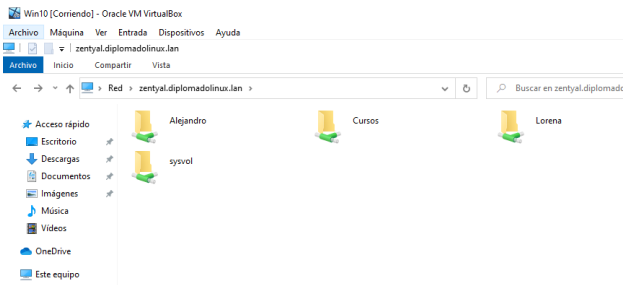


Imagen 63. Recursos compartidos en el dominio.

Se conecta un nuevo cliente Linux (Ubuntu) en el controlador de dominio a través de la aplicación pbis-open version 9.1.0.

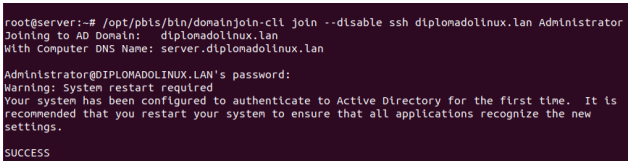


Imagen 64. Instalación paquetes Zentyal.

Se modifica el archivo 50-ubuntu.conf para permitir el inicio de sesión manual.

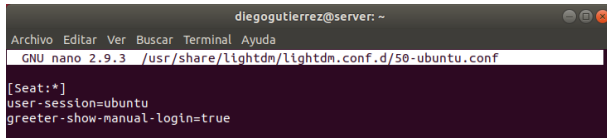


Imagen 65. Instalación paquetes Zentyal.

Finalmente se asigna una shell al usuario a través de la configuración de pbis-open.

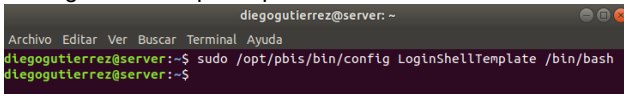


Imagen 66. Asignación shell.

Se procede a conectar el usuario juan@diplomado.lan y se verifica la conexión al dominio.

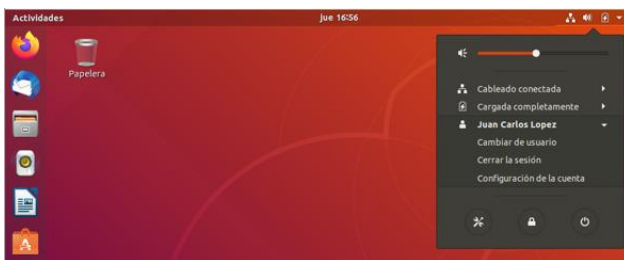


Imagen 67. Inicio de sesión en dominio

5 TEMÁTICA II: PROXY NO TRANSPARENTE

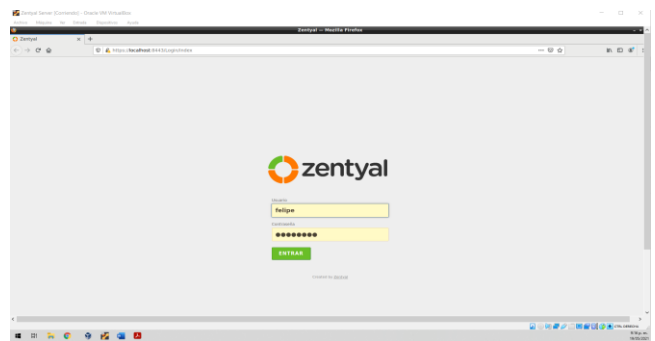


Imagen 68. Inicio sesión.

Se ingresa a la url dada por la distribución donde se procede a configurar de manera detallada el Proxy no transparente

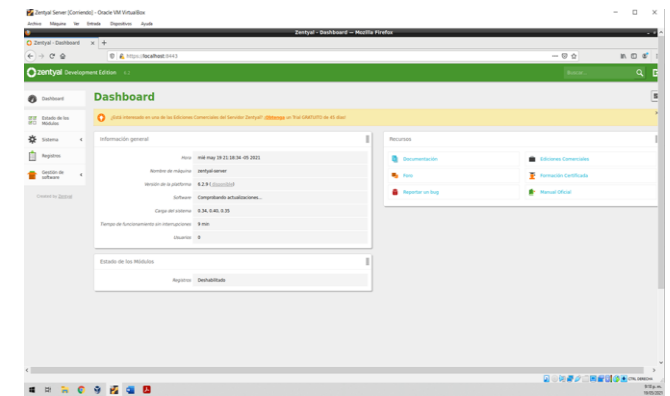


Imagen 69. Dashboard.

Se observa una correcta configuración del Zentyal Server

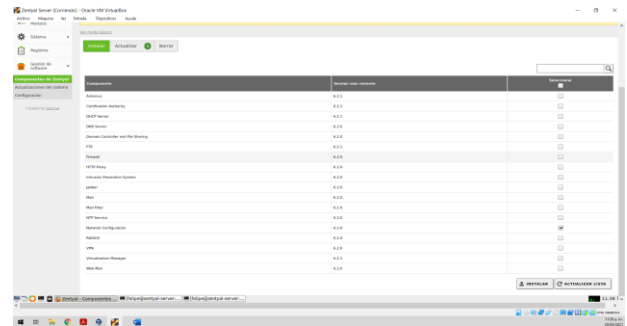


Imagen 70. Servidor.

Después de verificar que el servidor se conecta a Internet sin problema, se procede a instalar los paquetes de Network Configuration, Firewall y Http Proxy para proceder con la configuración respectiva.

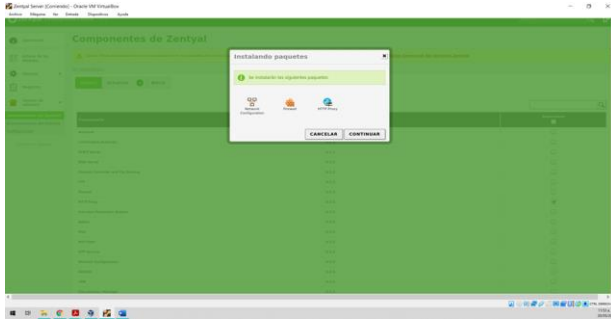


Imagen 71. Instalar paquetes.

Como se observa en la figura, se instalan los paquetes seleccionados

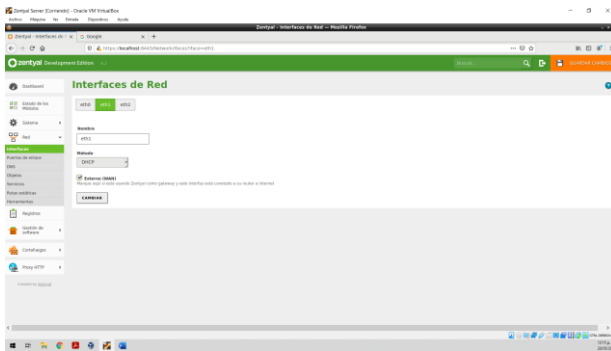


Imagen 72. Paquetes instalados.

En el módulo Red, se selecciona interfaces de Red, se modifica la interfase eth1 por WAN y método DHCP

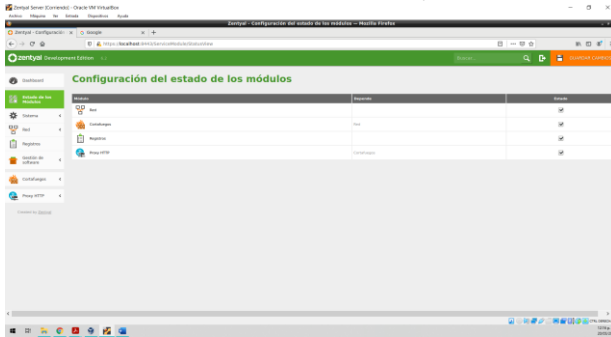


Imagen 73. Interfaces de red.

En la configuración del estado de los módulos, se habilita el Proxy HTTP

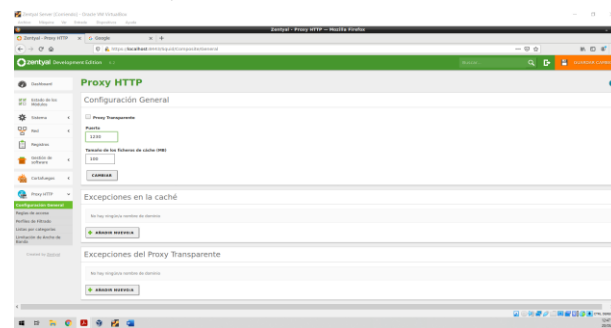


Imagen 74. Infraestructura tecnológica a la medida.

En el módulo Proxy HTTP, se ingresa el puerto N 1230 para filtrar la salida y conexión de Internet

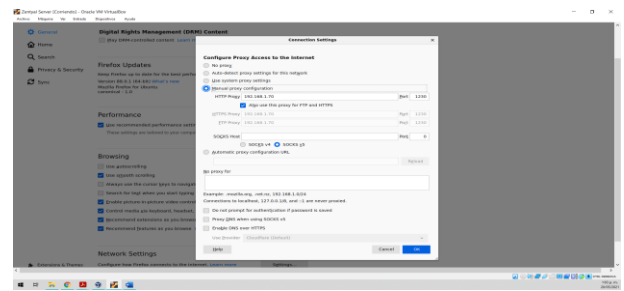


Imagen 75. Infraestructura tecnológica a la medida.

Como se observa en la figura, se cambia la configuración del Proxy a estado Manual 192.168.1.70 y puerto 1230

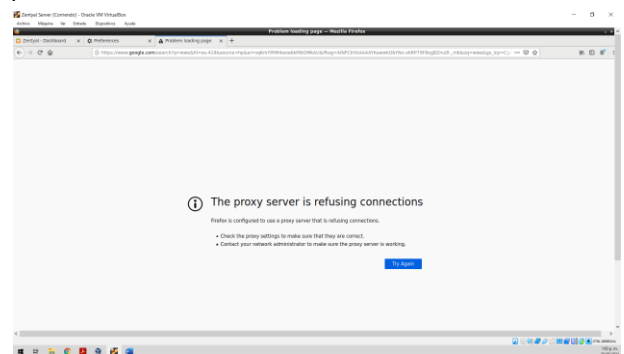


Imagen 76. Infraestructura tecnológica a la medida.

Se ejecuta la prueba de conexión y el navegador muestra que el proxy server está rechazando las conexiones



Imagen 77. Infraestructura tecnológica a la medida.

Como se observa en la figura, después de cambiar la configuración del proxy, el servidor se conecta sin problema a Internet.

6 TEMÁTICA III: CORTAFUEGOS

Inicialmente se instala en componentes de Zentyal el módulo de configuración de red, se asigna al adaptador de red LAN una IP estática, se asignó la IP 192.168.0.10 para el servidor, para poder conectar desde equipos cliente.



Imagen 78. Configuración IP estática.

Es necesario posteriormente realizar la instalación del módulo de servidor DNS, para poder controlar y resolver las peticiones de los equipos clientes.

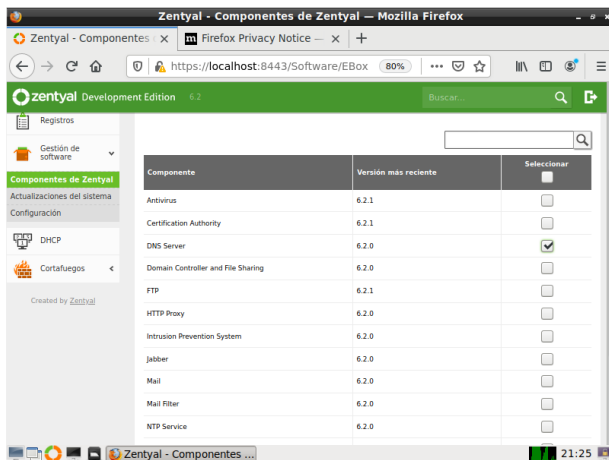


Imagen 79. Instalación servicio DNS

Se realiza de igual manera la instalación de módulo de servicios DHCP, para que les asigne IP dinámica a los equipos clientes, de igual manera se instala el firewall y se activan los módulos en Estado de los módulos.



Imagen 80. Activación de módulos

Se realiza la configuración DHCP, para establecer las direcciones IP dinámicamente. Se asigna el nombre DHCP y el rango disponible para los equipos de la red desde la 192.168.0.20 a la 192.168.0.100

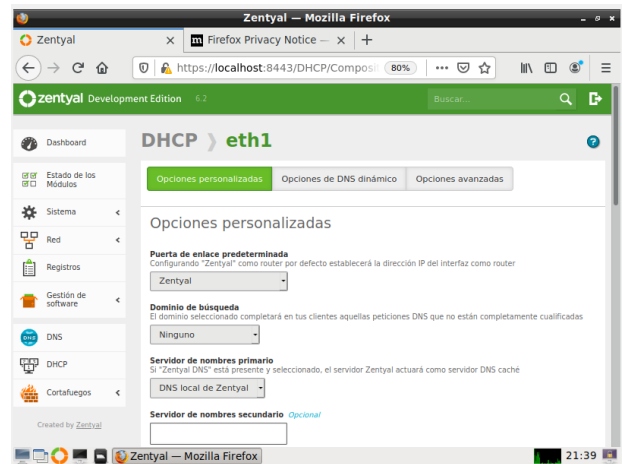


Imagen 81. Configuración DHCP

Una vez activado el servicio DHCP en el cliente en este caso es Ubuntu, se verifica en la terminal ejecutando el comando ifconfig, y se puede observar que le fue asignada la IP 192.168.0.20, para posteriormente realizar ping al servidor.

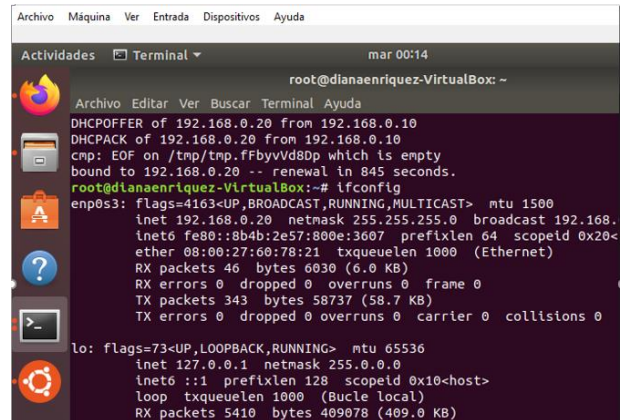


Imagen 82. Comprobación IP en equipo cliente

Una vez configurada la red, se procede a agregar las reglas del firewall que permitirán controlar el acceso a las diferentes redes sociales, en la ruta cortafuegos, filtrado de paquetes, reglas de filtrado, estas reglas internas, controlarán el tráfico de internet para bloquear el acceso a las redes sociales o cualquier página

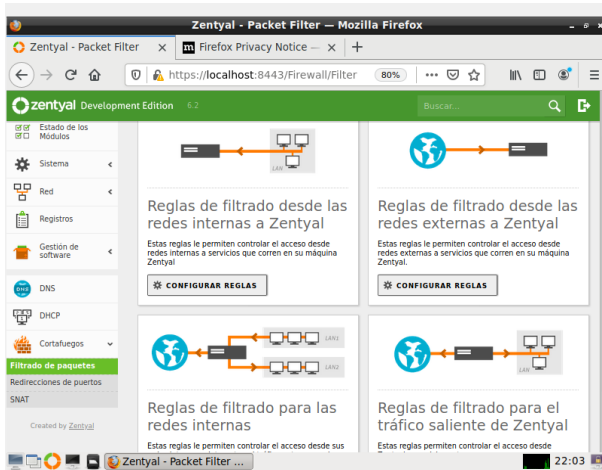


Imagen 83. Interfaz reglas de filtrado firewall

Se puede verificar que se puede navegar por la página de Facebook sin problema en el equipo cliente

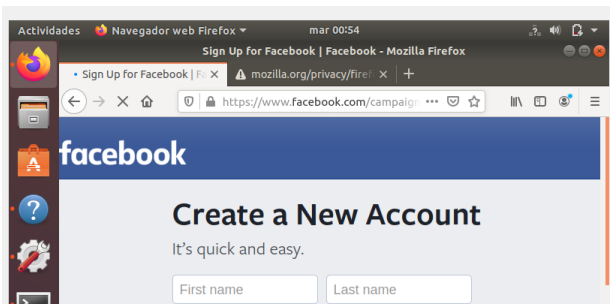


Imagen 84. Verificación inicial conexión a Facebook

Es necesario obtener la dirección IP de Facebook, la cual se obtiene con el comando ping www.facebook.com.

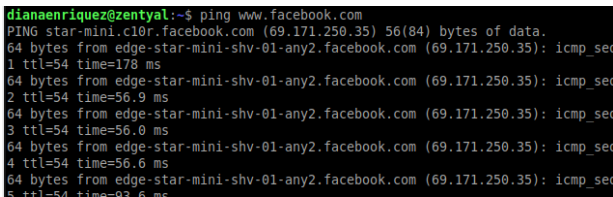


Imagen 85. IP Facebook

Se añade la regla donde se especifica que se deniega el acceso a la IP 69.171.250.35, correspondiente a Facebook, desde cualquier origen es decir cliente, de esta manera se bloquea y se realiza el mismo procedimiento con los protocolos http y https, y se guardan los cambios

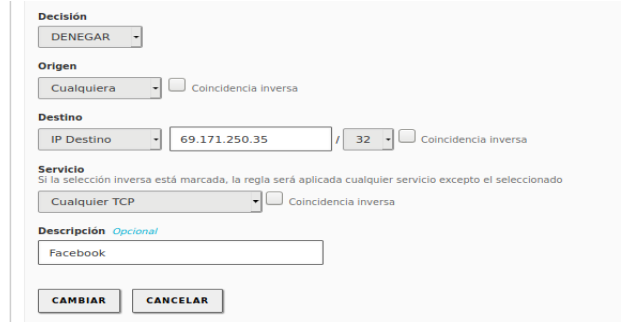


Imagen 86. Regla para denegar acceso a Facebook

Es necesario que las reglas se apliquen a todos los protocolos HTTP y HTTPS.

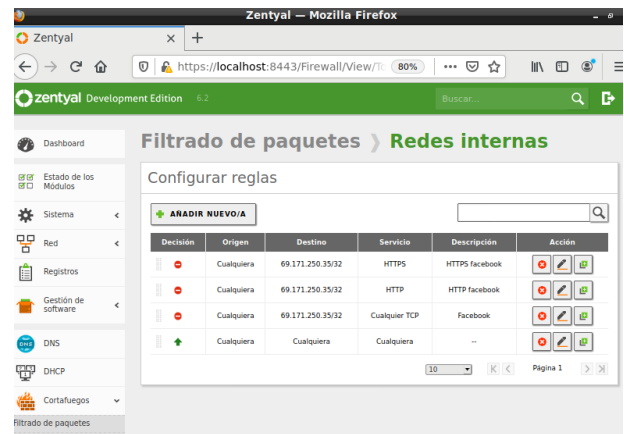


Imagen 87. Regla para protocolos Facebook

Ahora se comprueba en el equipo cliente, que efectivamente no se tiene acceso a la red social facebook, bloqueando los puertos de acceso desde el servidor Zentyal.

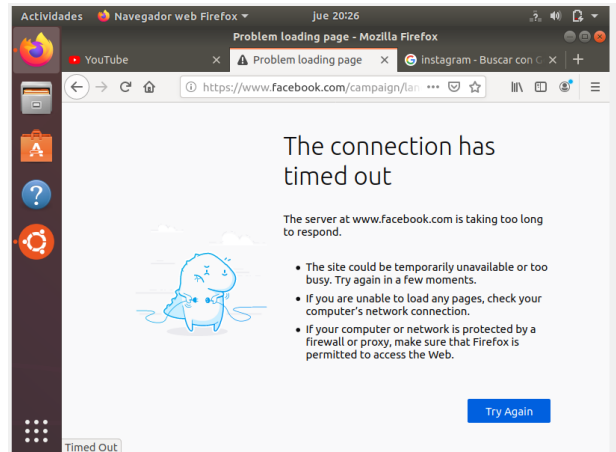


Imagen 88. Comprobación acceso denegado para Facebook

Se realiza el mismo procedimiento para YouTube se verifica la conexión y se obtiene dirección IP.

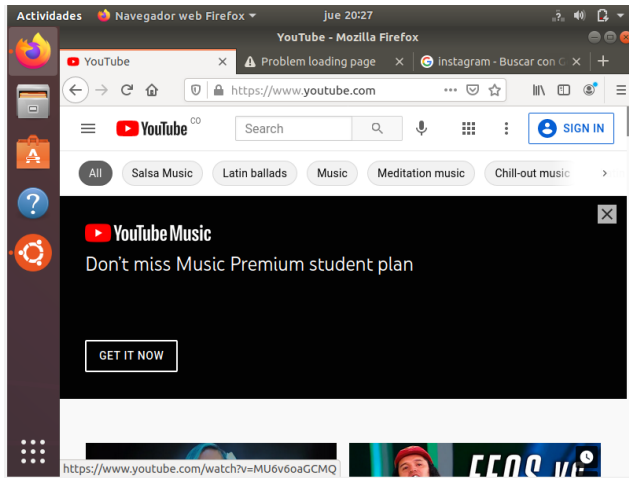


Imagen 89. Verificación inicial conexión a YouTube

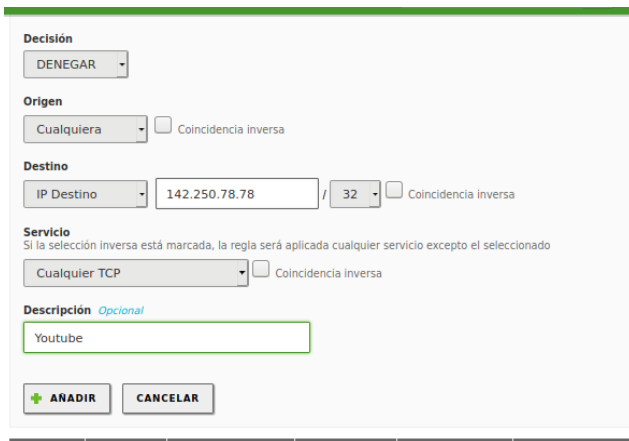


Imagen 90. Regla para denegar acceso a YouTube

Decisión	Origen	Destino	Servicio	Descripción	Acción
Denegar	Cualquiera	142.250.78.78/32	HTTPS	HTTPS youtube	[Iconos de configuración]
Denegar	Cualquiera	142.250.78.78/32	HTTP	HTTP youtube	[Iconos de configuración]
Denegar	Cualquiera	142.250.78.78/32	Cualquier TCP	Youtube	[Iconos de configuración]
Denegar	Cualquiera	69.171.250.35/32	HTTPS	HTTPS facebook	[Iconos de configuración]

Imagen 91. Regla para protocolos YouTube

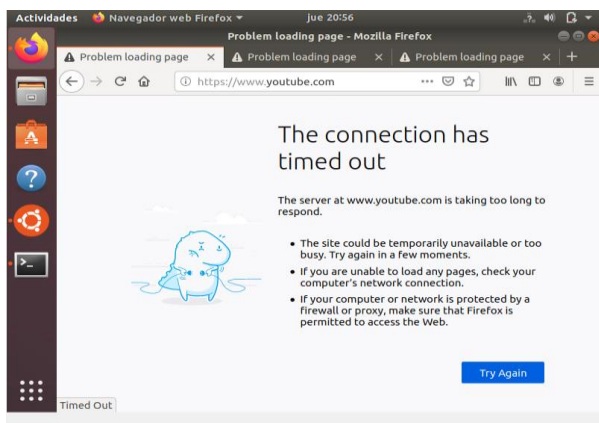


Imagen 92. Comprobación acceso denegado para YouTube

Se realiza el mismo procedimiento para la red social Instagram

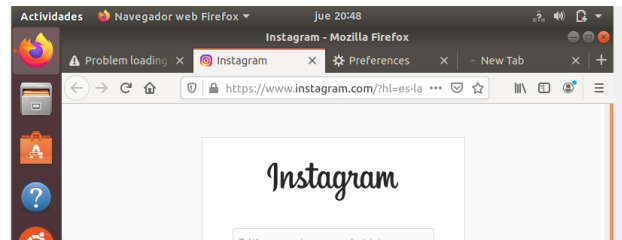


Imagen 93. Verificación conexión a Instagram

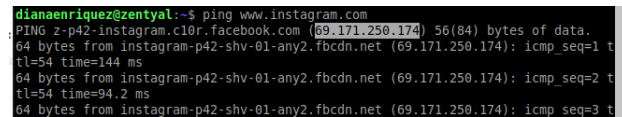


Imagen 94. Instagram

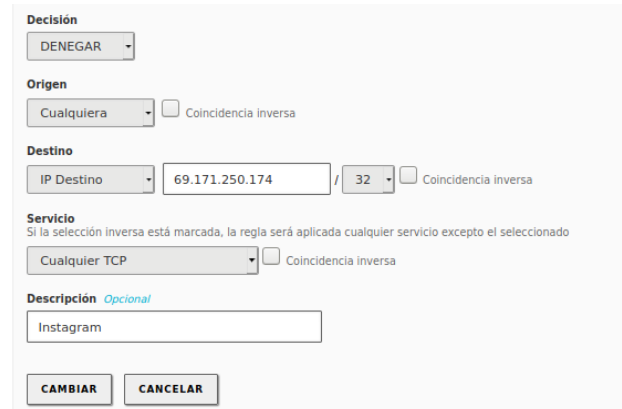


Imagen 95. Regla para denegar acceso a Instagram

Decisión	Origen	Destino	Servicio	Descripción	Acción
Denegar	Cualquiera	69.171.250.174/32	HTTPS	HTTPS instagram	[Iconos de configuración]
Denegar	Cualquiera	69.171.250.174/32	HTTP	HTTP instagram	[Iconos de configuración]
Permitir	Cualquiera	Cualquiera	Cualquiera	--	[Iconos de configuración]
Denegar	Cualquiera	69.171.250.174/32	Cualquier TCP	Instagram	[Iconos de configuración]
Denegar	Cualquiera	142.250.78.78/32	HTTPS	HTTPS youtube	[Iconos de configuración]

Imagen 96. Regla para protocolos Instagram

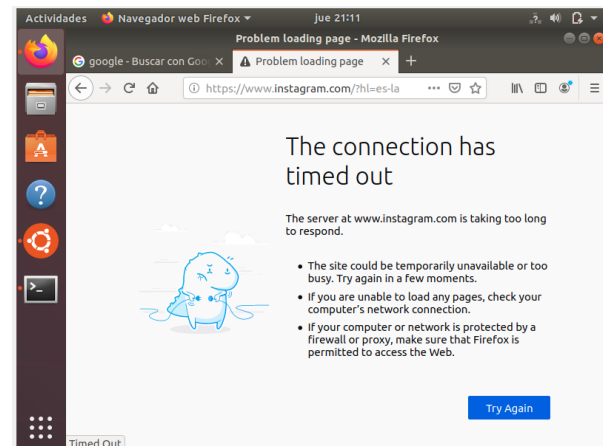


Imagen 97. Comprobación acceso denegado para Instagram

7 TEMÁTICA IV: FILE SERVER Y PRINT SERVER

Chequeo de módulos, se verifica que el módulo Controlador de Dominio y Ficheros este activo:

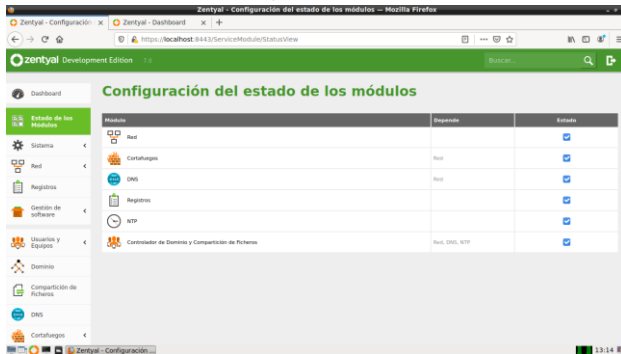


Imagen 98. Estado de los módulos

Configuración de Dominio: En el módulo de Dominio se agrega el nombre de Dominio y se completa los campos, luego se guardan los cambios:

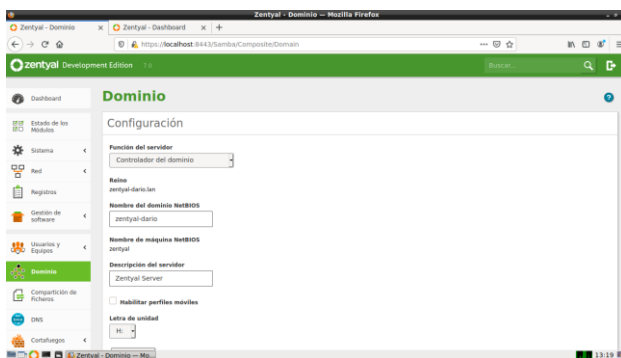


Imagen 99. Configuración de dominio

Configuración de Grupo y Usuario: En el apartado Usuarios y Equipos, se da clic sobre Gestionar y luego en el árbol se selecciona Groups y en la parte inferior se da clic en + para agregar un Grupo.

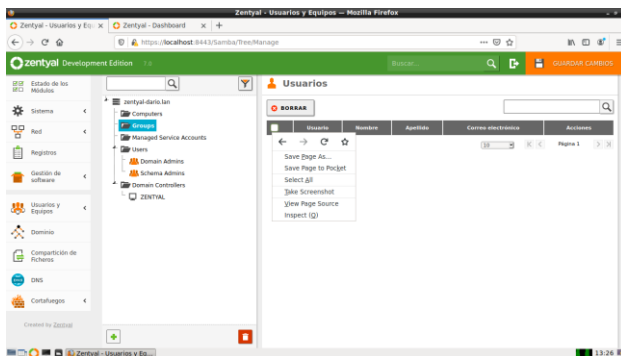


Imagen 100. Modulo de Compartición de Ficheros.

Se digita el nombre del grupo, en este caso "Diplomado-2021"

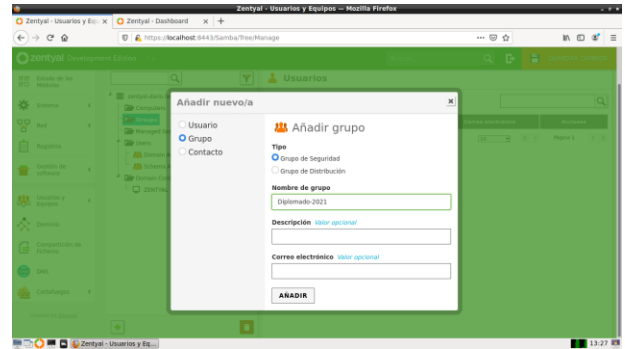


Imagen 101. Creando grupo

Se realiza el mismo proceso anterior para crear un Usuario, solo que esta vez en el árbol se selecciona Users y se completa los campos correspondientes, teniendo en cuenta seleccionar el grupo anteriormente creado.

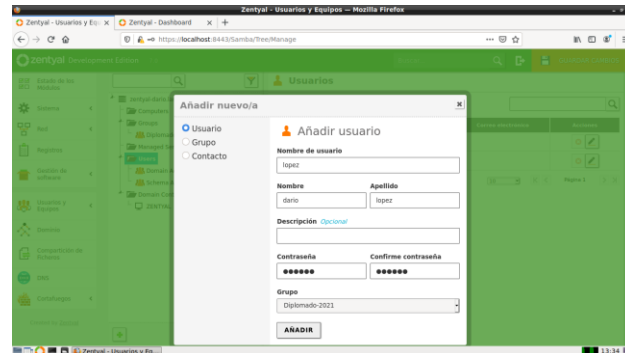


Imagen 102. Creando Usuario.

Creando fichero compartido y configurando acceso: En Compartición de Ficheros se da clic en Añadir Nuevo/a y se digita los datos del recurso y finalmente clic en Añadir:

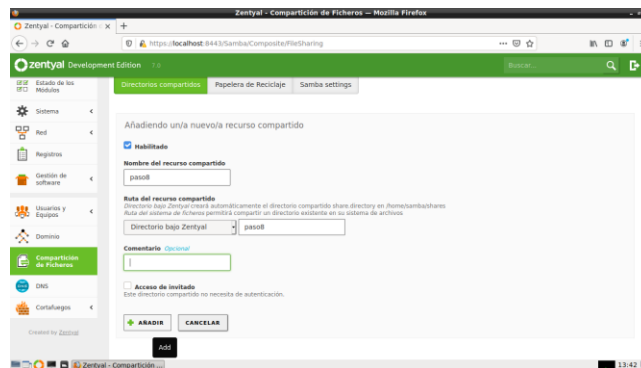


Imagen 103. Creando recurso.

Después, en control de Acceso, se da clic en Añadir Nuevo/a, se selecciona el Usuario y se proporciona los permisos respectivos, finalizado el proceso se da clic en Añadir.



Imagen 104. Otorgando permisos

En este punto se dirige a la maquina Ubuntu y en Archivos se da en conectar al servidor, digitando smb://192.168.10.1 y clic en conectar:

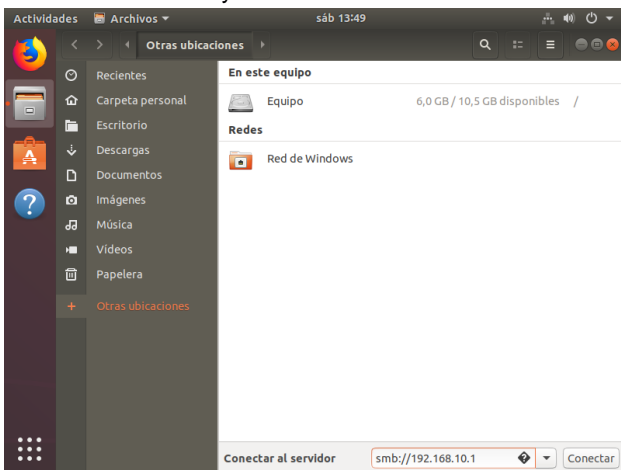


Imagen 105. Conectando al servidor

Al tratar de ingresar solicita las credenciales por lo que se procede a digitarlas y dar clic en conectar:

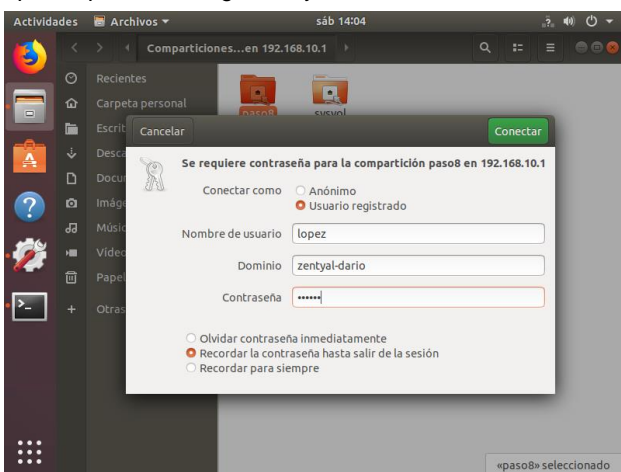


Imagen 106. Autenticación

Como se puede apreciar se ha logrado acceder con éxito al recurso compartido.

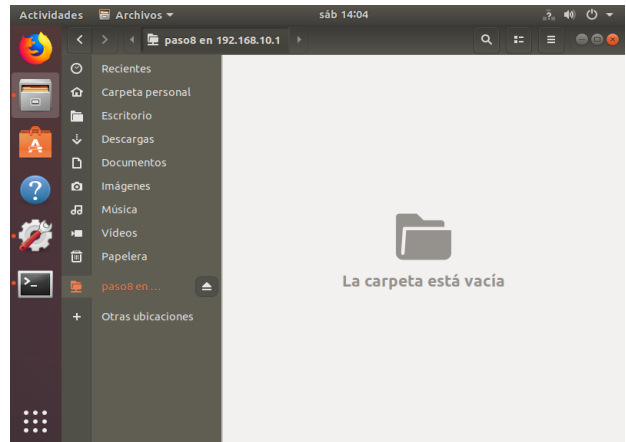


Imagen 107. Ingresando a carpeta compartida.

Para configurar y compartir la impresora, se necesita hacer uso de CUPS, ya que el administrador de impresoras dejó de estar disponible a partir de Zentyal 5. Por ello procede a instalarlo con `sudo apt install cups`.

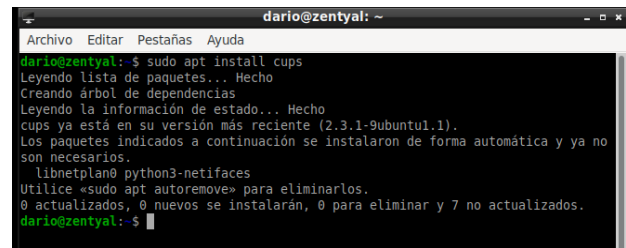


Imagen 108. Instalando CUPS.

Ahora se instala CUPS-PDF para hacer uso de una impresora virtual, con `sudo apt install cups-pdf`.

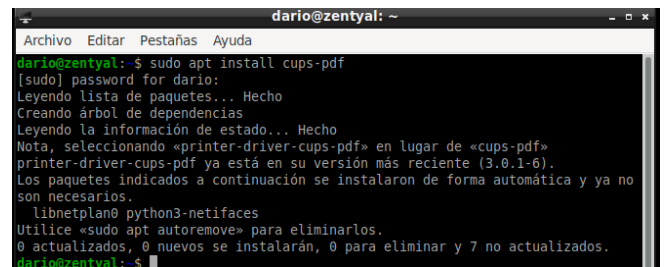


Imagen 109. Instalación CUPS-PDF.

Ahora se accede a cups mediante localhost:631, en administración se dar a Add Printer para agregar la impresora:

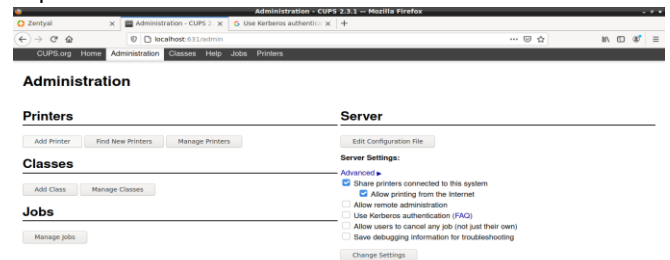


Imagen 110. Interfaz web de CUPS.

Se da el nombre de "Dario_PDF" a la impresora y se activa la casilla de compartición:



Imagen 111. Añadiendo Impresora.

Se Selecciona un driver genérico:

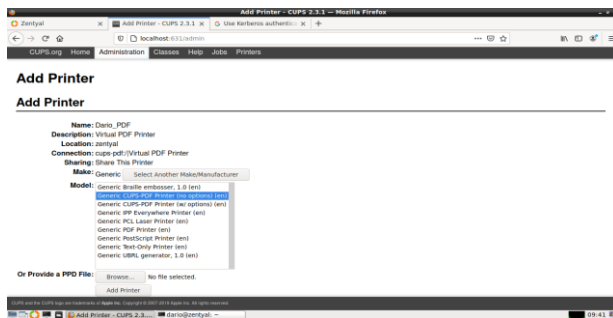


Imagen 112. Configurando el Driver.

Finalmente, la impresora queda instalada y a la escucha:



Imagen 113. Instalación completada.

Se procede a ir a la maquina Ubuntu, en impresoras, en la pestaña servidor, se digita la IP de Zentyal y se puede ver la impresora compartida, se da clic en ella para agregarla:

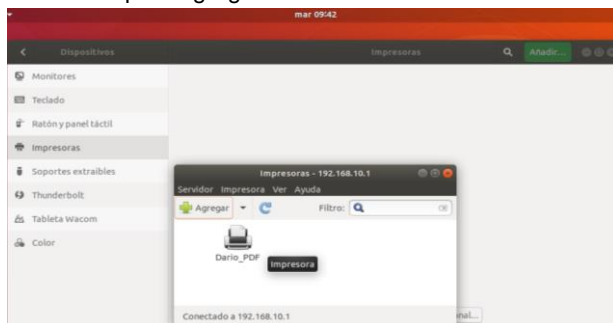


Imagen 114. Añadiendo impresora.

Una vez en la configuración se da "imprimir página de prueba" para cerciorarse de que está funcionando:

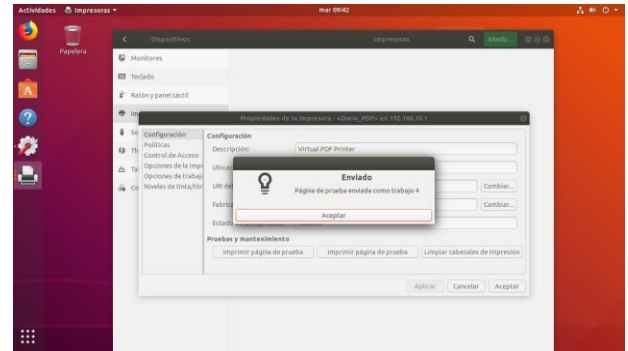


Imagen 115. Realizando impresión de prueba.

En el servidor se puede ver que el trabajo se realizó correctamente:

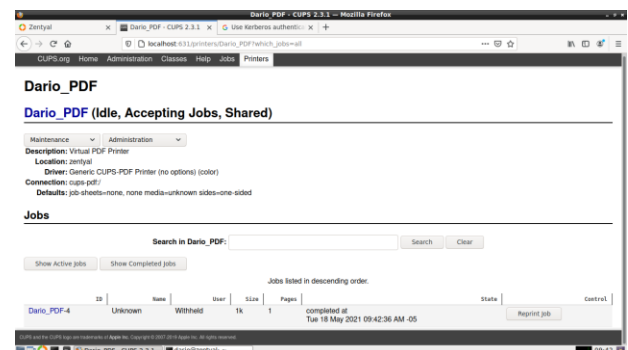


Imagen 116. Verificando en el servidor.

8 TEMÁTICA V: VPN

Lo primero que se debe hacer es ingresar a Gestión de software a la opción de componentes de Zentyal y se selecciona para instalar el módulo de VPN.

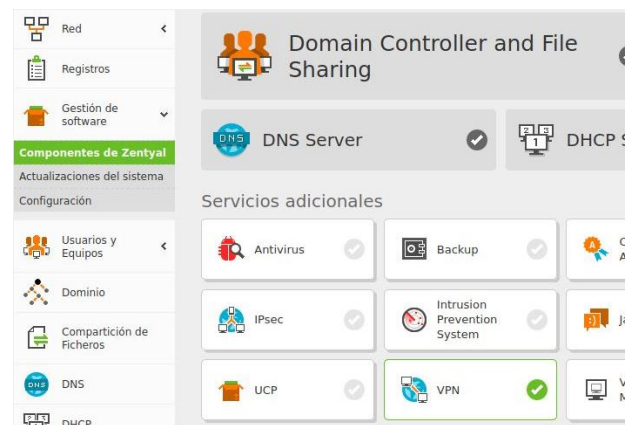


Imagen 117. Módulo VPN

S da continuar para instalar el Modulo de VPN y el Certification Authority.

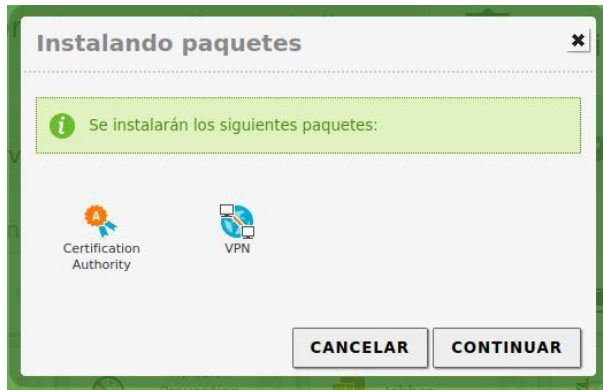


Imagen 118. Instalar paquetes VPN

Se empiezan a instalar los paquetes de los módulos seleccionados.

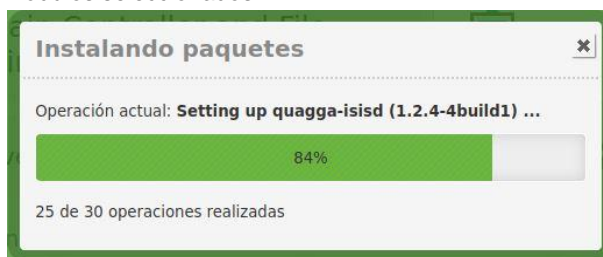


Imagen 119. Instalando VPN

Finaliza la instalación de los paquetes y se da clic en OK.

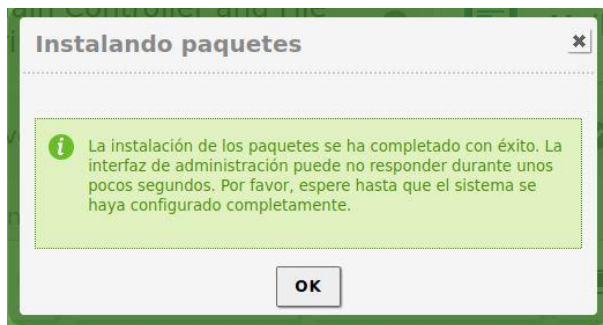


Imagen 120. VPN Instalada

Se ingresa a la opción "VPN" y en la sección Servidores, allí se presiona en la opción "Añadir Nuevo".

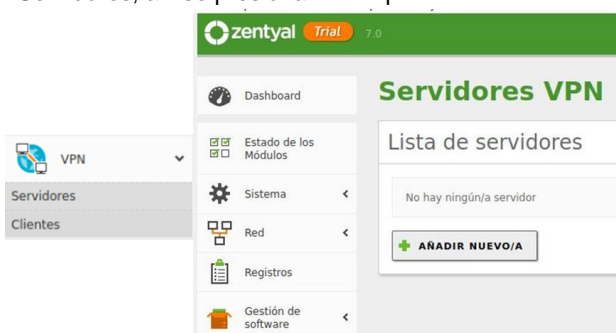


Imagen 121. Servidores

Se establece el nombre del servidor de VPN para este caso "MiguelZentyal".



Imagen 122. Servidor VPN

Se ingresa al módulo de Autoridad de Certificación y pestaña – General y se crea un certificado para la conexión con el servidor.

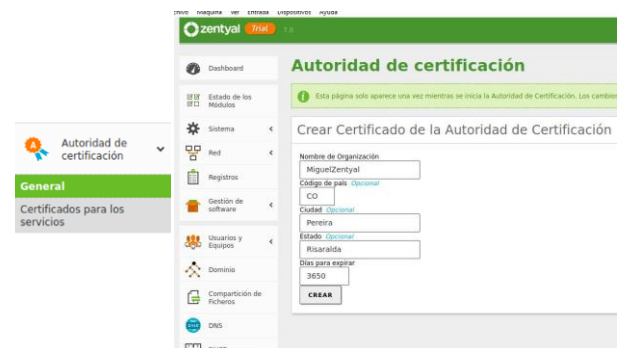


Imagen 123. Certificado VPN

Con esto ya se tiene creado el certificado de conexión el cual se descargará posteriormente para instalarlo en el equipo cliente desde el cual se conectará por VPN al servidor.

Lista de Certificados actual

Nombre	Estado	Fecha	Acciones
MiguelZentyal Authority Certificate desde MiguelZentyal	Válido	2031-05-18 00:53:17	[Iconos de acciones]
vpn-MiguelZentyal	Válido	2031-05-18 00:53:17	[Iconos de acciones]

Imagen 124. Listado Certificados VPN

En el Módulo de Servidores VPN y en el listado se ingresa a la opción de Configuración.



Imagen 125. Configurar

En la configuración se indica el Puerto como UDP y se deja por defecto en 1194, se indica una segmentación de red para que esta sea entregada por la VPN en el momento de la conexión.



Imagen 126. Configurar servidor VPN

Luego en la sección de Red en la casilla servicios, para crear el servicio de la VPN en la Red y se da clic en añadir.

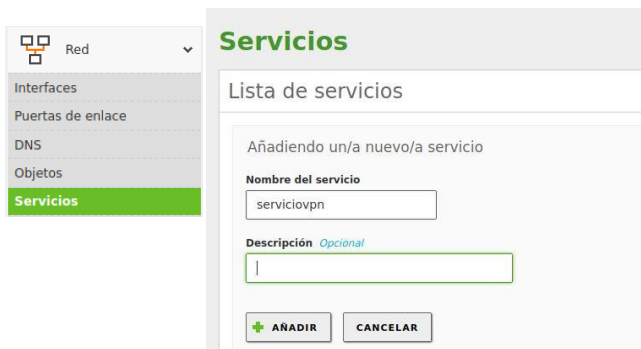


Imagen 127. Configurar servidor VPN

Allí se asocia el protocolo de conexión UDP al servicio de la VPN en la red con puerto de destino, ya asociado anteriormente al servidor.



Imagen 128. Servicio VPN

Posteriormente en el módulo de Cortafuegos se configurar el filtrado de paquetes para que cuando se establezca la conexión a la VPN desde un cliente externo este no sea bloqueado y permita la conexión, así que se ingresa al Filtrado de paquetes y se da clic en configurar reglas.



Imagen129. Packet Filter

Allí se crea la regla indicando aceptar las conexiones desde cualquier origen que use el servicio de red de VPN asociado que ya se creó llamado "ServicioVPN" y se agrega una descripción y se da en "Añadir".



Imagen 130. Filtrado

Se Debe conocer la IP publica de acceso para el servidor de la VPN esto se puede hacer ingresando por ejemplo a una página como who.is y allí mostrará la IP Pública, 186.83.194.147 para este caso.



Imagen 131. IP Pública

Se verifica con Ifconfig la conexión de red actual de del servidor, se encuentra una dirección IP para la WAN, otra IP de distinto segmento para la LAN, la IP por defecto para el localhost 127.0.0.1 y finalmente el segmento de red entregado por la VPN configurado previamente.

```

miguel_herrera@miguelserv: ~
Archivo Editar Pestañas Ayuda
miguel_herrera@miguelserv: $ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.0.13 netmask 255.255.255.0 broadcast 192.168.0.255
    ether 08:00:27:8a:7c:d3 txqueuelen 1000 (Ethernet)
    RX packets 12727 bytes 14557444 (14.5 MB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 10270 bytes 806076 (800.6 KB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

eth1: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.1.10 netmask 255.255.255.0 broadcast 192.168.1.255
    ether 08:00:27:54:94:39 txqueuelen 1000 (Ethernet)
    RX packets 0 bytes 0 (0.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 72 bytes 7920 (7.9 KB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    loop txqueuelen 1000 (Local Loopback)
    RX packets 28569 bytes 3290110 (3.2 MB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 28569 bytes 3290110 (3.2 MB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

tap0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.160.1 netmask 255.255.255.0 broadcast 192.168.160.255
    ether b2:ca:e6:da:6b:e3 txqueuelen 100 (Ethernet)
    RX packets 0 bytes 0 (0.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 0 bytes 0 (0.0 B)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

miguel_herrera@miguelserv: $

```

Imagen 132. Red del servidor

Con esto ya se finaliza la configuración del servidor, ahora se debe preparar la conexión por medio del cliente que va a usar la VPN.

Se entra a los servidores de VPN, se escoge el servidor "MiguelZentyal" y se ingresa en la opción Descargar paquete de configuración del cliente.

Allí se exporta el certificado para conexión del cliente así que se indica el tipo de cliente que se va a conectar, se selecciona para este caso conectar una máquina en Windows, para mirar compatibilidad entre sistemas operativos, ya que hasta el momento todos los clientes han sido Linux, también se indica en el certificado del cliente a que servidor va a conectarse, y en la dirección del servidor se pone la IP Pública, esto para que sirva desde cualquier red externa y finalmente en la Dirección IP adicional se pone la IP local del servidor. Se puede seleccionar incluir el instalador de Open VPN en el paquete de configuración a exportar, pero para este caso se descargará aparte para observar el paso a paso.



Imagen 133. Exportar configuración

Allí el servidor entrega un archivo .zip con el certificado y toda la configuración de conexión.

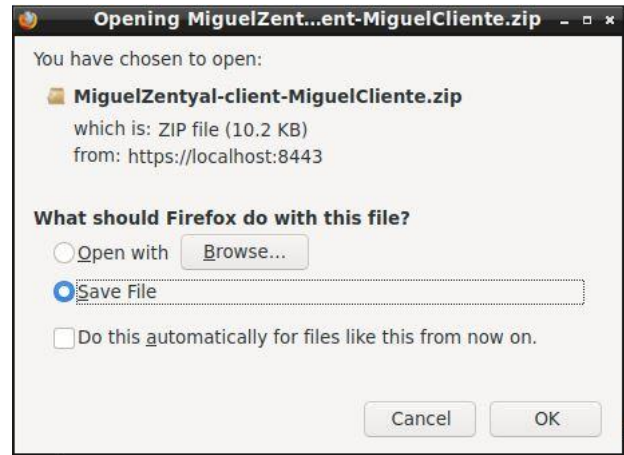


Imagen 134. Paquete de configuración

Este paquete de configuración se envía a la máquina cliente por medio de un correo electrónico colocándolo en los archivos adjuntos.

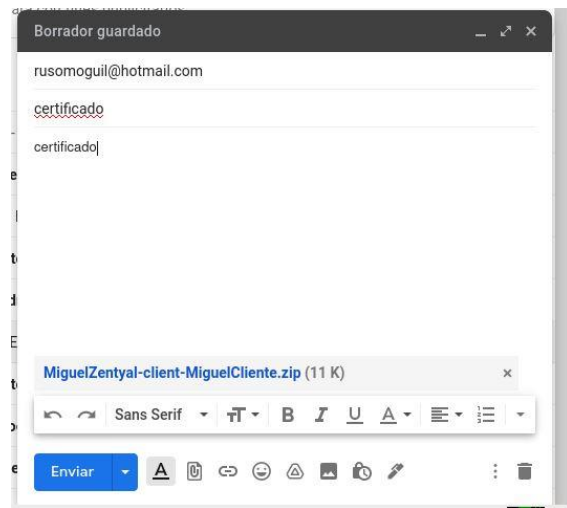


Imagen 135. Envío

En el equipo cliente se procede a entrar a la página de OpenVPN y se descarga el archivo instalador para proceder con la instalación del mismo.

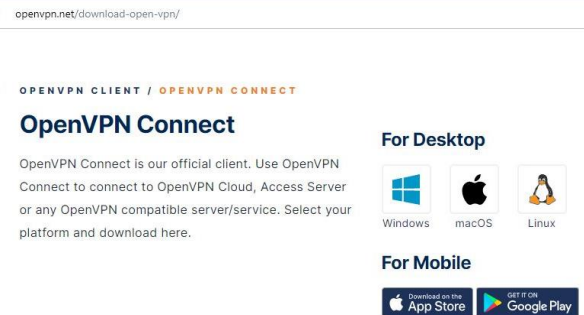


Imagen 136. OpenVPN

Se descarga el archivo instalador y se procede a instalar el aplicativo OpenVPN.

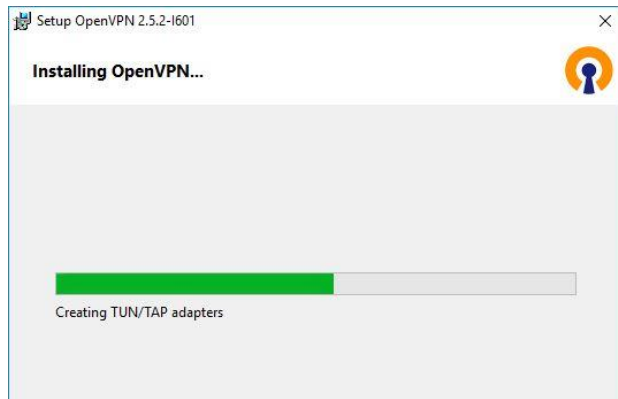


Imagen 137. Instalando OpenVPN

Una vez acabe la instalación se encuentra en el escritorio el icono del software ya instalado.



Imagen 138. OpenVPN Instalado

Se ubica el paquete de instalación en el archivo .zip descargado y se descomprime.

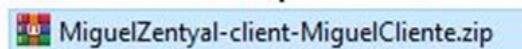


Imagen 139. Paquete de configuración

Se seleccionan todos los archivos resultantes al descomprimir el archivo de configuración .zip y se copian para pegarlos en otra ubicación.

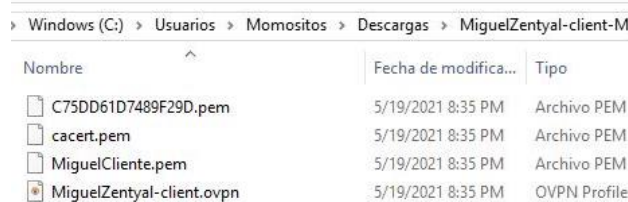


Imagen 140. Descomprimido

Se va a la Carpeta principal de instalación de OpenVPN en la carpeta Config y se pegan los archivos.

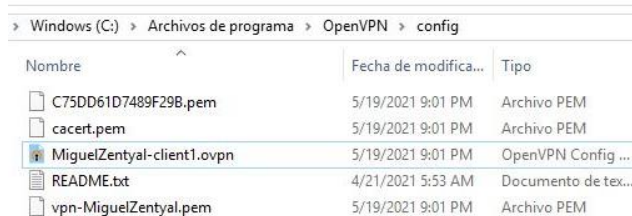


Imagen 141. Pegado de archivos

Posteriormente se va al icono del software OpenVPN ya instalado y ejecutado; Se indica Importar un archivo, allí se debe seleccionar el archivo con extensión .ovpn que es el certificado de conexión al servidor Zentyal, de allí importará toda la configuración de conexión previamente configurada.

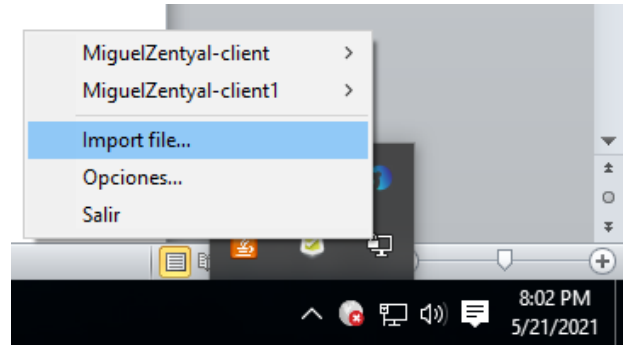


Imagen 142. Importar archivo

Si todo sale bien el software OpenVPN indicará que el certificado fue correctamente importado.

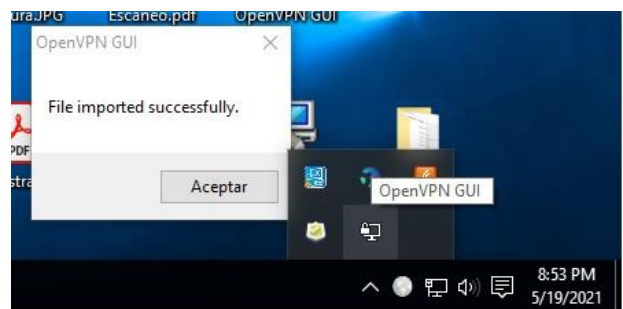


Imagen 143. Archivo Importado

Se da clic, entonces en el programa Open VPN se selecciona el Certificado importado y se da clic sobre la opción "Conectar"

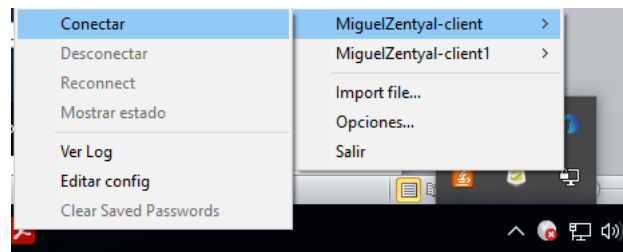


Imagen 144. Conectar

Allí se observa un recuadro con todo el proceso de conexión del cliente a la VPN del servidor Zentyal.

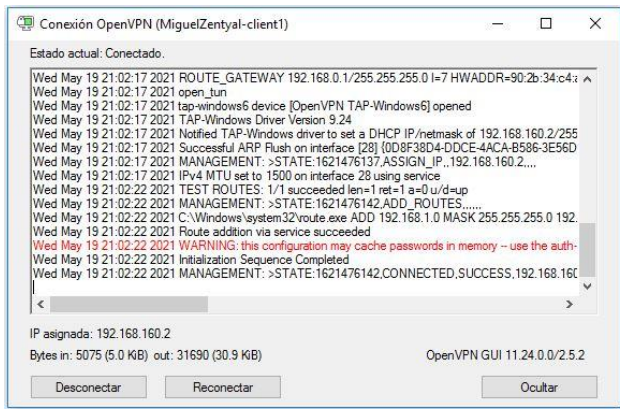


Imagen 145. Conectado

En la imagen anterior se puede apreciar el estado actual: Conectado y en la parte de abajo indica la IP asignada por el servidor VPN Zentyal al cliente, 192.168.160.2 para este caso, también saldrá el siguiente recuadro indicando que se conectó correctamente a la VPN del servidor con la IP asignada.

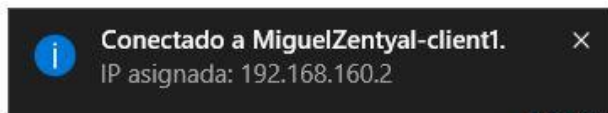


Imagen 146. Conectado al server

Después de estar conectado, se puede hacer IPConfig para verificar la IP asignada por el servidor VPN al equipo cliente 192.168.160.2 y también la IP local de conexión que le entrega el adaptador de red de internet.

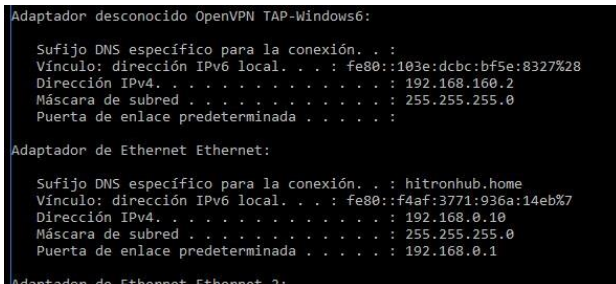


Imagen 147. Red del cliente

Si se realiza un ping a la dirección IP de destino del servidor VPN se puede ver que responde sin inconveniente desde la IP Pública.

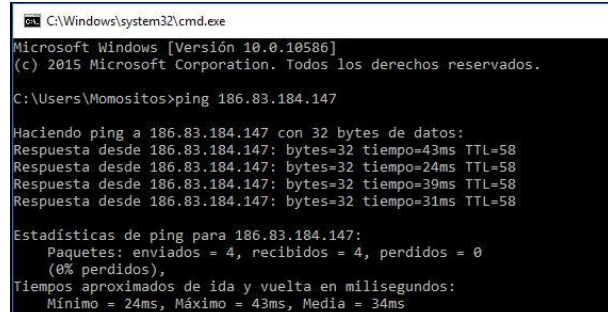


Imagen 148. Ping

También se puede enviar paquetes con respuesta correcta al servidor no solo a través de su conexión de red establecida LAN sino también desde su red y segmento entregado por la VPN.

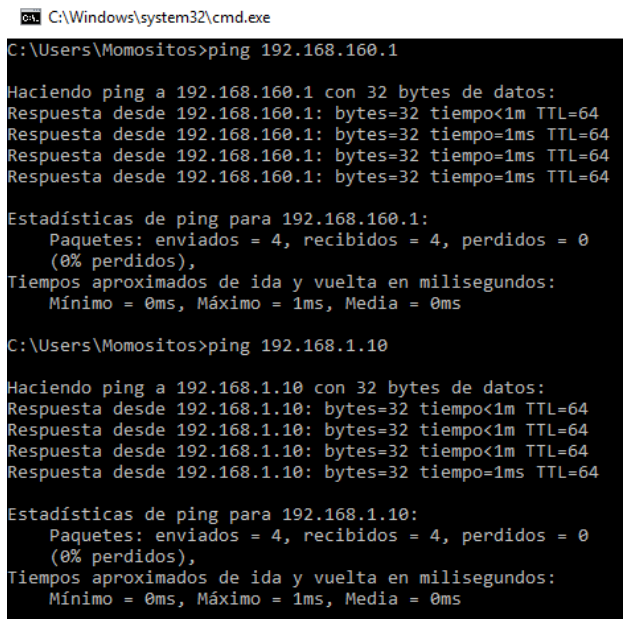


Imagen 149. Ping entre redes

Después de que la conexión desde el cliente se realizó sin inconveniente, se ingresa al servidor Zentyal para verificar la conexión activa desde el equipo cliente.

Se ingresa al panel de Zentyal y en el Dashboard se verifica que el servicio de conexión VPN está habilitado y ejecutándose, allí se verifica la conexión por el servicio y en el puerto UDP 1194, a través de que dispositivo de red VPN recibe la conexión (tap0) y la segmentación de red entregada a los clientes.



Imagen 150. Servicios VPN

9 CONCLUSIONES

Zentyal Server facilita la gestión de infraestructura IT a través de un entorno gráfico y un asistente de configuraciones, facilitando la implementación de servicios como DHCP, DNS, controlador de dominio, Gateway entre otros servicios, siendo una alternativa Linux que puede reemplazar los servicios prestados por Windows Server a un precio mucho más bajo.

Gracias al módulo de Compartición de Ficheros la tarea de compartir recursos en red se convierte en una tarea amena. Se pueden crear grupos y usuarios para tener un mayor control de la infraestructura. En cuanto al servidor de impresión a pesar de no existir un módulo dedicado se puede realizar esta tarea gracias a CUPS.

Zentyal ofrece soluciones de control de tráfico para las redes internas y redes externas, por medio de asignaciones sencillas de reglas en la configuración del cortafuegos, de esta manera se puede aceptar o denegar las conexiones, realizando un filtro en las páginas a las que los clientes pueden acceder, evitando la saturación y peligros en la red.

El módulo de conexión de servicios de VPN del servidor Zentyal ofrece soluciones de conectividad a diversos clientes y sistemas operativos, este genera conexión fácil a través del servicio VPN con direccionamiento tanto público como local, entregándoles IPs con segmentación previamente definida en el servidor a través del TAP del adaptador VPN, la conexión es establecida con el certificado y configuración exportada desde el mismo servidor usada posteriormente a través del software intuitivo y de fácil uso - OpenVPN.

Zentyal permite configurar de manera satisfactoria un Proxy no transparente a través de sus servicios y módulos del servidor, los servicios de navegación restringida para Infraestructura IT aplicándolos en la navegación de la manera que deseamos.

10 REFERENCIAS

- [1] Murillo, R. (2020, 20 mayo). Zentyal 6.2: Instalación y Configuración - Parte #1 [Video]. YouTube. <https://www.youtube.com/watch?v=gJYJm2vxbc>
- [2] Zentyal (2018). Documentación Zentyal. <https://doc.zentyal.org/6.2/es/>
- [3] Castel, A. (2018, 3 diciembre). Unir Ubuntu 16.04 a Dominio Linux con Zentyal. Blog d'Alex Castel. <https://alexcastel.wordpress.com/2018/12/03/unir-ubuntu-16-04-a-dominio-linux-con-zentyal/>
- [4] Zentyal Community (2021), Documentación de Zentyal 7.0 – Instalación. <https://doc.zentyal.org/es/installation.html#el-instalador-de-zentyal>

- [5] Campos, R. (2019), Instalación de Zentyal Server 6 en VirtualBox. [Archivo de Video]. Youtube. <https://www.youtube.com/watch?v=T2Db4DF1yao>
- [6] Phikev (2020), Failed to Parse .OVPN File, TAP Mode Not Supported. <https://forums.openvpn.net/viewtopic.php?f=29&t=31398>
- [7] ProngerTV (2020) Cómo instalar y configurar un servidor VPN en Zentyal - Tutorial 2020. [Archivo de Video]. Youtube. <https://www.youtube.com/watch?v=8zaxU1C7qBc>
- [8] Rodriguez, R. (2015) Configuración y conexión a un servidor VPN con Zentyal usando OpenVPN. [Archivo de Video]. Youtube. <https://www.youtube.com/watch?v=3rNfipxE-9o>
- [9] Morales, H. Restrepo, I. Ardila, A. Muriel, L. Umbarila L. (2021) Diplomado de Profundización en Linux (Opción de trabajo de grado) 201494-7 TC8. Implementación y Administración de un Servidor Zentyal, [Archivo PDF]. <https://repository.unad.edu.co/bitstream/handle/10596/23431/idrestrepov.pdf?sequence=1&isAllowed=y>