

TRABAJO FINAL, PASO 8, SOLUCIONANDO NECESIDADES ESPECÍFICAS CON GNU/LINUX, GRUPO 8

Jonathan Moncada
e-mail: j.moncada.ramirez27@gmail.com
Johana Alexandra Salcedo Cortés
e-mail: johanasalcedo316@gmail.com
John Jairo Yara
e-mail: yarkjj@gmail.com
Oscar Javier Parra
e-mail: ojparraa@unadvirtual.edu.co
Rafael Andrés Bernal
e-mail: digired33@gmail.com

RESUMEN: En el presente trabajo se pretende realizar la administración y control de una distribución GNU/Linux basada en Ubuntu, pero enfocada a la implementación de servicios de infraestructura IT de mayor nivel para Intranet y Extranet en instituciones complejas. Para ello se utiliza Zentyal como sistema operativo base para disponer de los servicios de esta Infraestructura IT, se implementan bajo Zentyal servicios DHCP Server, DNS Server, Controlador de Dominio, Proxy no transparente, Cortafuegos, File Server y Print Server. Dicha implementación se lleva a cabo desde la consola de Zentyal con configuraciones previas como zona DMZ de acuerdo con la Red administrable para acceder desde el GNU/Linux al Zentyal Server, se evidencia control y encaminamiento de la red, lo que significa que con Zentyal se logra reducir y racionalizar las TIC, mejorar la seguridad y minimizar los tiempos de inactividad del sistema.

PALABRAS CLAVE: administración, enrutamiento, seguridad, servidor.

1 INTRODUCCIÓN

Esta guía incluye las descripciones completas de los tipos de letra, del espaciado, y la información relacionada para elaborar sus reportes, basada en los formatos utilizados por la IEEE.

2 INSTALACION DE ZENTYAL

Creamos la máquina virtual asignando la ram y espacio en disco

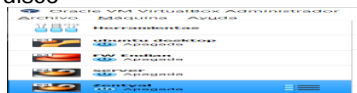


Fig. 1 Partición máquina virtual

Luego cargamos el disco a instalar e iniciamos el proceso de instalación



Fig. 2 Seleccionando idioma

Seleccionamos la primera opción de la instalación



Fig. 3 Opción de instalación.

Luego de configurar opciones básicas del sistema como el idioma y el teclado debemos configurar las interfaces.

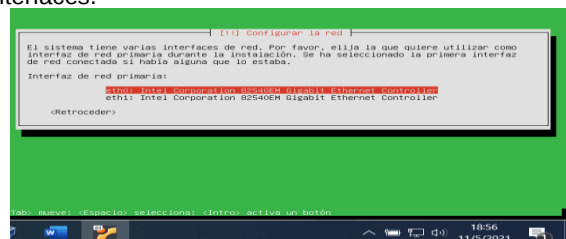


Fig. 4 Configurar tarjetas de red.

Nombramos la máquina, creamos un usuario y agregamos una contraseña de acceso.

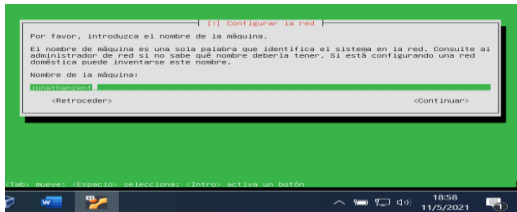


Fig. 5 Configurando datos del sistema.

Confirmamos que la configuración de reloj sea la correcta.

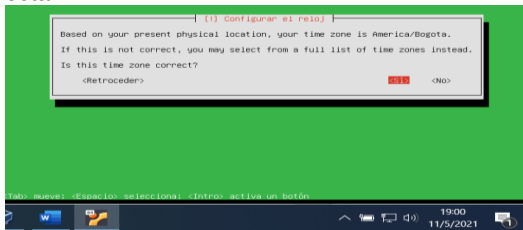


Fig. 6 Configuración del reloj.

Esperamos que el proceso de instalación finalice.

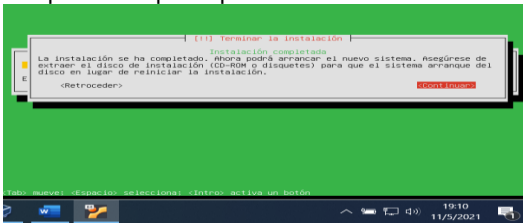


Fig. 7 finalización de la instalación.

3 TEMÁTICAS

3.1 DHCP Server, DNS Server y Controlador de Dominio

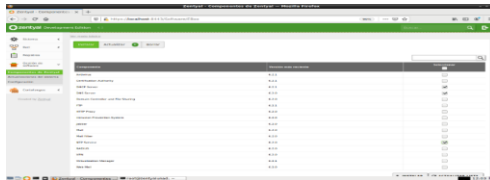


Fig. 8 Instalación de servicios DNS SERVER, DHCP SERVER.

Se procede a realizar la instalación del software para implementar los servicios de DHCP server, DNS server, desde el panel de administración de Zentyal.

3.1.1 SERVIDOR DNS

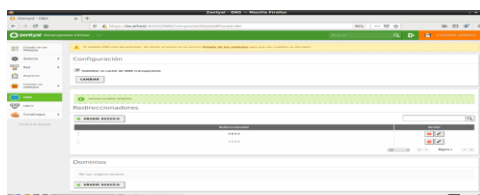


Fig. 9 Configurando DNS SERVER.

Se habilita el caché DNS transparente y se agregan al redireccionado de DNS servidores de DNS, como el 8.8.8.8 y 1.1.1.1 de Google.

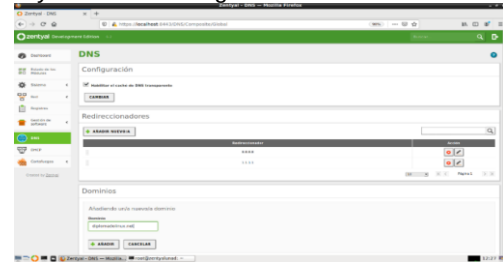


Fig. 10 Cambio de dominio.

Se procede a realizar cambio del dominio en el módulo DNS SERVER, en el que se especifica que el dominio será diplomadolinux.net.

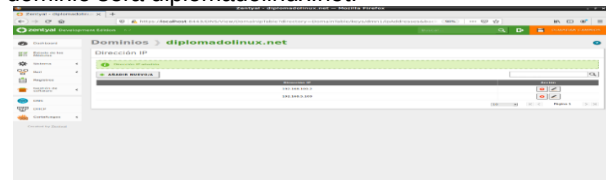


Fig. 11 Eliminando dirección interfaz Wan de direcciones Ip del dominio

Se procede a ingresar a las direcciones Ip del dominio para eliminar la dirección Ip de la interfaz Wan, ya que solo será utilizada para la interfaz de red interna.



Fig. 12 prueba de resolución de nombres en navegador equipo cliente.

Como prueba se realiza conexión a través de navegador de equipo cliente.

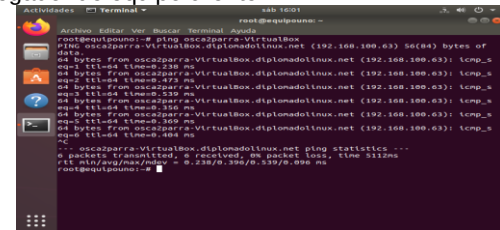


Fig. 13 Prueba de resolución de nombres en terminal equipo cliente.

Se realiza prueba desde terminal equipo cliente realizando ping a otro equipo conectado a la red.

3.1.2 SERVIDOR DHCP

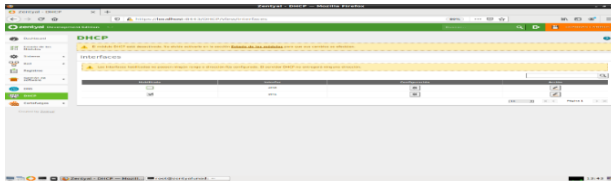


Fig. 14 Habilitando DHCP server para interfaz interna.

Se habilita el servicio DHCP que se va a configurar solo para la interfaz Eth1 la cual es la asignada para la red interna.

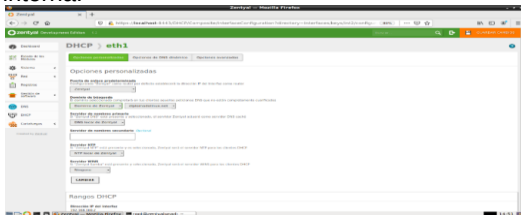


Fig. 15 Configurando opciones personalizadas interfaz Eth1.

Se establece en opciones personalizadas de la interfaz eth1 la puerta de enlace, el dominio de búsqueda, el servidor de nombres primario asignado para el servidor Zentyal.

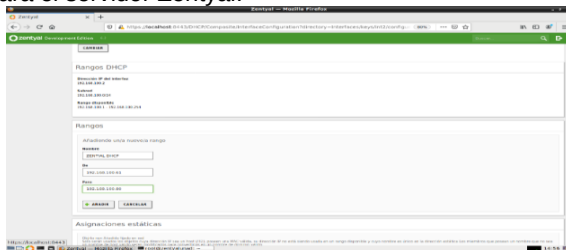


Fig. 16 Configurando Rangos de asignación DHCP

Se configuran los rangos de asignación de IPS por medio de DHCP, como se configuraron dos segmentos de direcciones IP según los objetos creados se crean estos dos rangos.

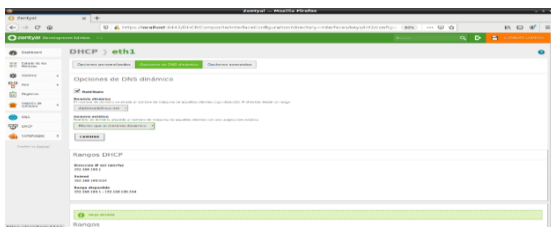


Fig. 17 Configurando Rangos de asignación DHCP

Se habilita en opciones de DNS Dinámico, el dominio dinámico seleccionando el dominio creado para la red.

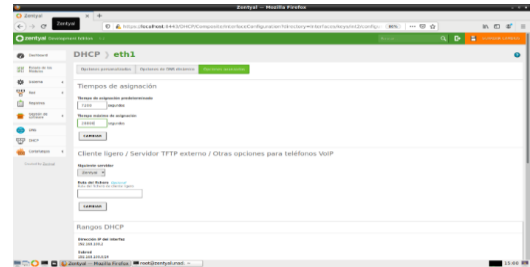


Fig. 18 Configurando tiempos de asignación.

Se realiza configuración de los tiempos de asignación en este caso se establece 7200 segundos para tiempo predeterminado de asignación y 28800 para tiempo máximo de asignación de direcciones IP.

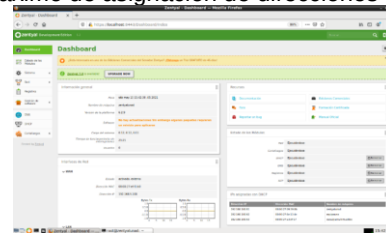


Fig. 19 información en Dashboard IPS asignadas

Se comprueba en el Dashboard las Ips que se están asignando de forma dinámica, se puede observar que se están asignando 3 IPS: 192.168.100.61, 192.168.100.62 y 192.168.100.63.

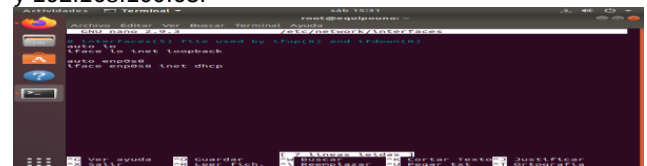


Fig. 20 Configuración DHCP en equipo cliente

Para que el equipo cliente tome la dirección que le asigna el servidor DHCP, se debe crear la línea iface enp0s8 inet dhcp, en el archivo interfaces, donde enp0s8 es la tarjeta de red que tiene comunicación con el servidor.

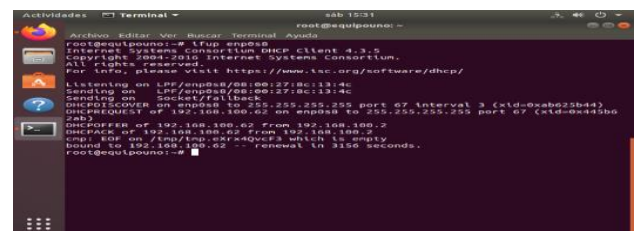


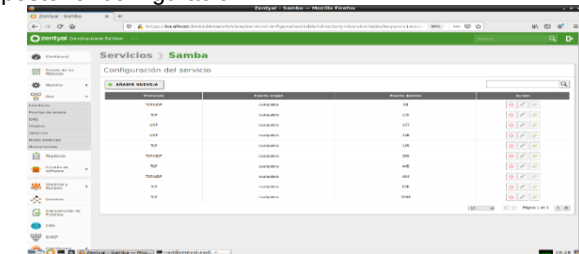
Fig. 21 servicio DHCP establecido a equipo cliente

Se comprueba que el servicio DHCP es efectivo en el equipo cliente como en la imagen indica se le ofrece la dirección 192.168.100.62 desde la dirección 192.168.100.2 la cual es la dirección IP del servidor DHCP.

3.1.3 CONTROLADOR DE DOMINIO



Se selecciona el paquete de software Domain Controller and file sharing para realizar su instalación y posterior configuración.



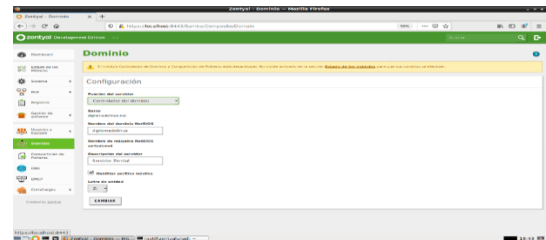
Se observa la configuración predeterminada que presenta el servicio Samba después de la instalación del paquete de software Domain Controller and file sharing.



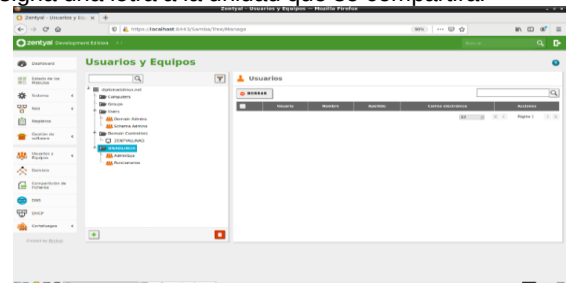
Fig. 24 Creando reglas en firewall redes internas para servicio Samba



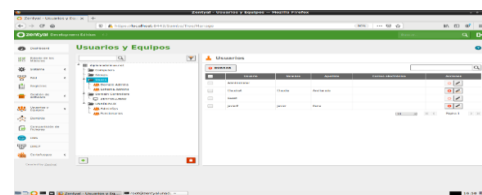
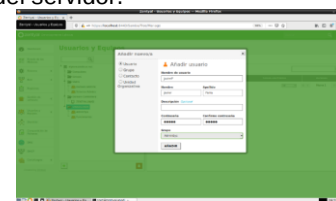
Se visualiza las reglas creadas en Firewall para el servicio Samba entre los objetos creados para la red.



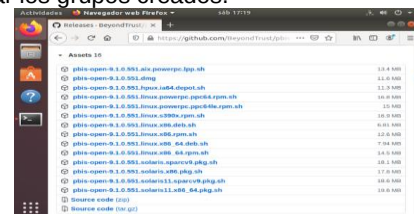
Al configurar el controlador de dominio se establece en función del servidor Controlador de dominio, se digita el nombre del dominio, se habilita perfiles móviles, y se asigna una letra a la unidad que se compartirá.



Se procede a crear los usuarios de dominio con los cuales se podrá ingresar a los equipos que se incluyan en el dominio del servidor.



En la sección de Users se puede visualizar los usuarios que se han creado en UNADLINUX se puede visualizar los grupos creados.



Se descarga de la página <https://github.com/BeyondTrust/pbis-open/releases>, el complemento .deb que corresponde a la distribución de Linux del equipo cliente en el cual se ingresara al dominio el servidor.

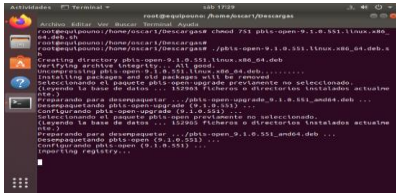


Fig. 31 instalación de archivo pbis-open-9.1.0.551.linux.x86_64.deb.sh

Se cambian los permisos sobre el archivo pbis-open-9.1.0.551.linux.x86_64.deb.sh; descargado previamente y se procede a ejecutar la instalación del software pbis-open.

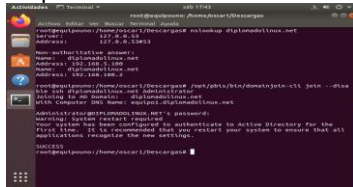


Fig. 32 Configurando equipo al dominio del servidor

Se procede a agregar el equipo al dominio con la instrucción `/opt/pbis/bin/domainjoin-cli join --disable ssh diplomadolinux.net Administrator`, después de ejecutarla el sistema solicita el password de Administrator.

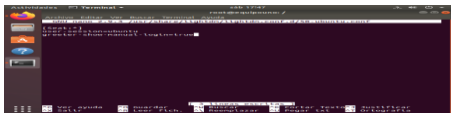


Fig. 33 Modificando archivo 50-ubuntu.conf

Se modifica el archivo `/usr/share/lightdm/lightdm.conf.d/50-ubuntu.conf`; con el fin de iniciar sesión con usuario de dominio y su clave después de reiniciar el equipo.



Fig. 34 ingresando con usuario de dominio al equipo cliente

Se ingresa el `usuariodedominio@dominio`, y posteriormente se digita la clave asignada a ese usuario.



Fig. 35 inicio de sesión con usuario de dominio.

Al abrir la terminal se comprueba que se ha iniciado sesión con el usuario JavierP dentro del dominio diplomadolinux.net.

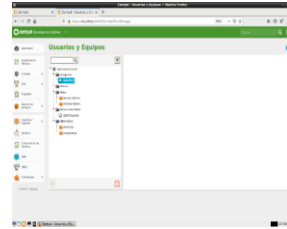


Fig. 36 Comprobación de equipo1 incluido en el dominio

Se comprueba en el panel del servidor la inclusión del equipo1 dentro del dominio de la red.

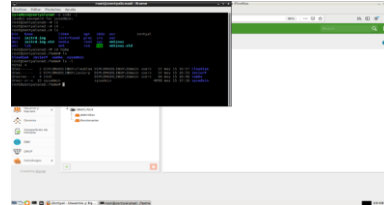


Fig. 37 Comprobación de los directorios creados en servidor.

Al crear los usuarios en el panel del servidor, se crean los directorios en el servidor en el directorio `/home`.

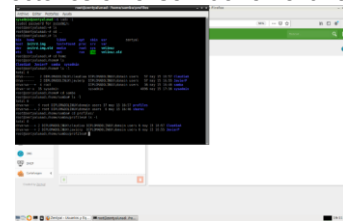


Fig. 38 Perfiles de usuarios en directorio samba.

Así mismo se puede comprobar que automáticamente se crean los perfiles de los usuarios en el directorio `/home/samba`.

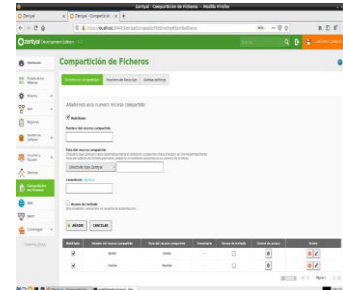


Fig. 39 configuración compartición de Ficheros.

Se realiza configuración de los ficheros compartidos creando los directorios a compartirse.

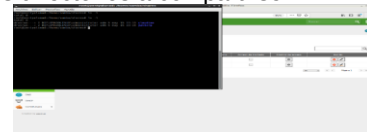


Fig. 40 Comprobación de directorios creados en servidor

Se comprueba que en el servidor se crean los directorios a compartirse en la ruta `/home/samba/share`.

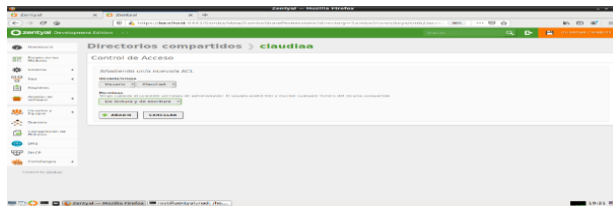


Fig. 41 Asignando permisos a usuarios sobre los directorios.

Se configuran los controles de acceso a los directorios compartidos, añadiendo usuarios o grupos al acceso a los directorios, en este caso se le otorga permiso de lectura y escritura al directorio claudiaa al usuario ClaudiaA.

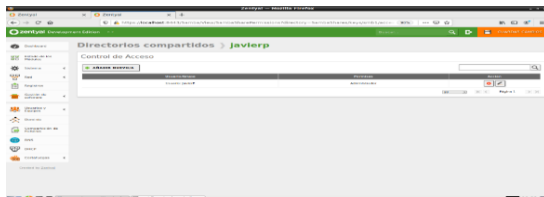


Fig. 42 Permisos sobre directorio javierp a usuario JavierP

En este caso al usuario JavierP se le otorgan permisos de administrador sobre el directorio javierp.

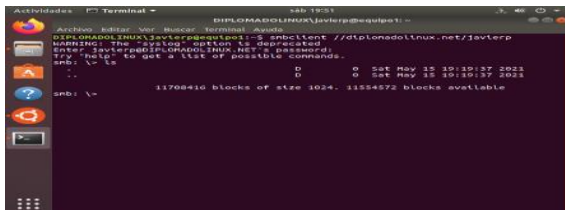


Fig. 43 ejecutando servicio samba cliente en equipo cliente

Se ejecuta instala smbclient con el comando apt-get install smbclient y se verifica el servicio con la configuración //diplomadolinux.net/javierp para verificar el estado y acceder a los ficheros compartidos a través del servicio Samba del servidor.

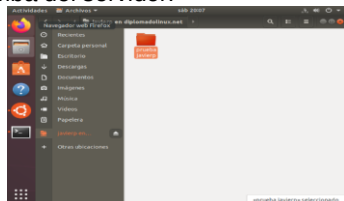


Fig. 44 Probando servicio de ficheros compartidos

Se prueba el servicio de ficheros compartidos y se crea un directorio de prueba en el fichero compartido.



Fig. 45 Directorio creado desde equipo1

Se comprueba la creación del directorio prueba javierp, el cual fue creado desde el usuario de dominio JavierP y su acceso al directorio javierp.



Fig. 46 Acceso directo a folder compartidos

Se comprueba que a través del usuario JavierP desde equipo1 se puede acceder a los folders compartidos a través del servicio Samba en el servidor.

3.2 PROXY NO TRANSPARENTE

Iniciamos la configuración del Zentyal, seleccionamos los paquetes que queremos instalar, para esta ocasión instalaremos varios, pero solo usaremos dos Network configuration y HTTP Proxy

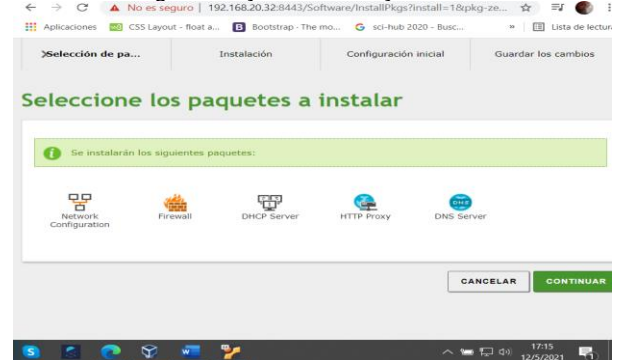


Fig. 47 Paquetes a instalar.

Luego de la instalación de los recursos a usar nos pedirá configurar las interfaces.

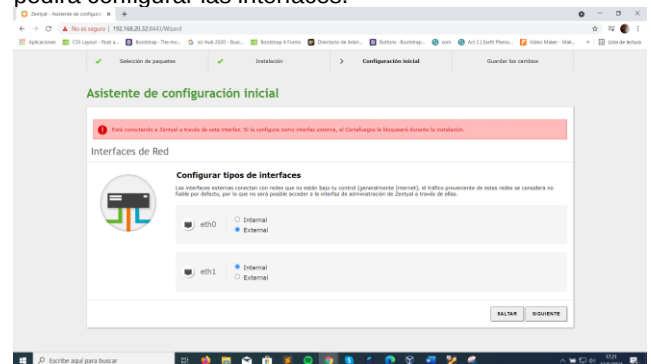


Fig. 48 configurar interfaces

Configuramos la primera interfaz que tiene salida a internet, acá no es importante si se configura por DHCP o estática.

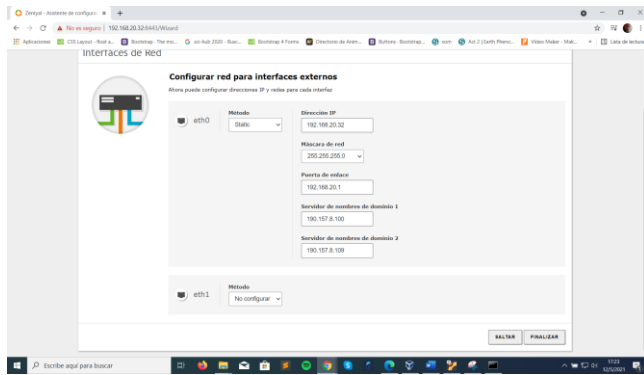


Fig. 49 configurar interfaz WAN

Para la interfaz que va hacia la LAN es importante dejarla estática ya que esta servirá como Gateway de nuestros equipos de la LAN.

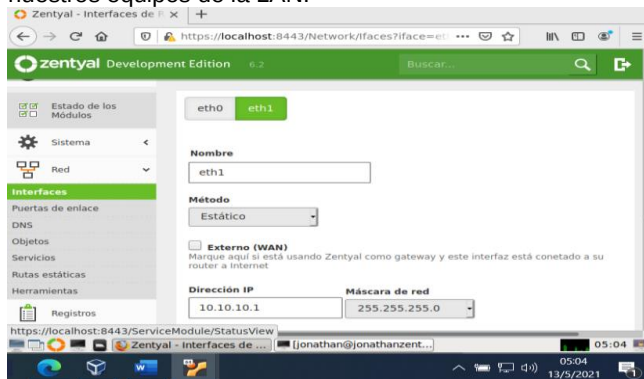


Fig. 50 Interfaz LAN

Debemos crear un objeto con el cual identificamos el grupo de equipos para la política que crearemos en el proxy.

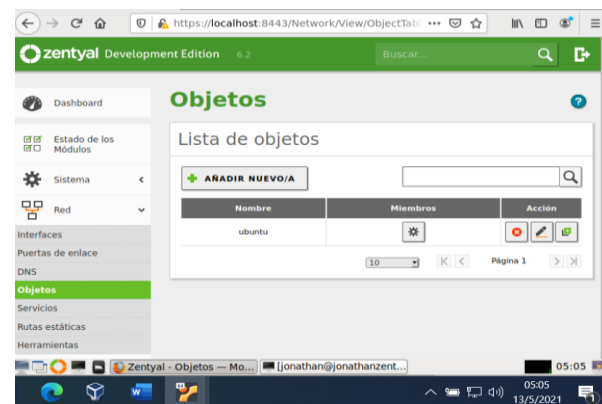


Fig. 51 creando objetos.

Dentro del objeto podemos agregar usuarios a los cuales queremos generar las restricciones o permisos de navegación según la regla.

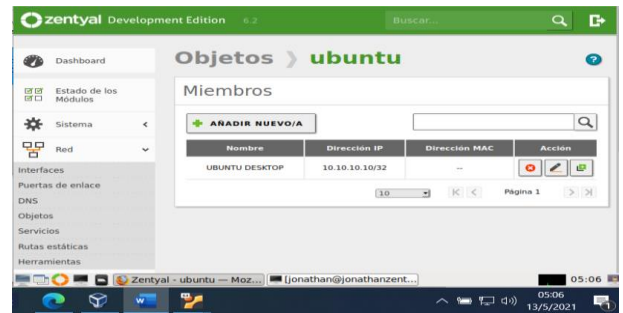


Fig. 52 agregando miembros

Vamos al menú de Proxy HTTP a la opción de configuración general, nos aseguramos de que la opción de proxy transparente esté desmarcada y agregamos el puerto.

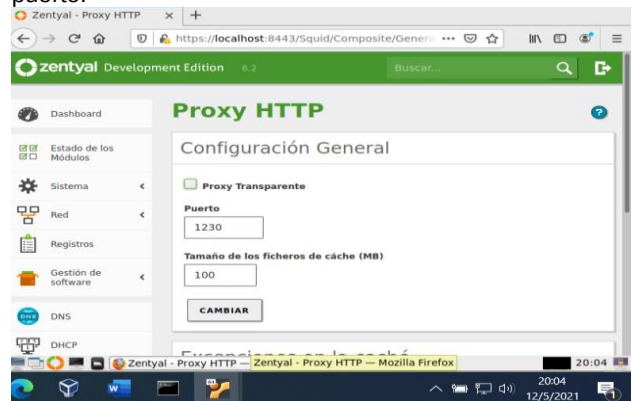


Fig. 53 configuración general del Proxy

Creamos una regla de acceso que se aplicara a nuestro proxy, recordemos que las reglas no son solo para denegar también se puede crear para permitir la navegación.

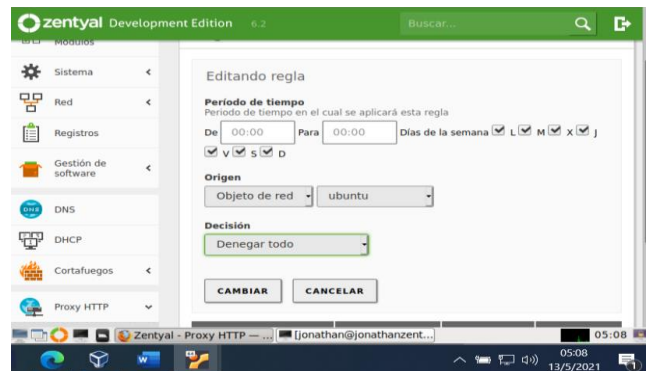


Fig. 54 creando regla de acceso

Y debemos asegurarnos que en la opción de módulos este activo nuestro Proxy.

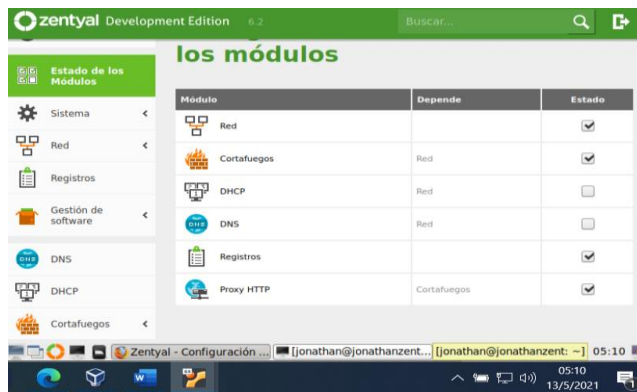


Fig. 55 confirmando modulo activo

Para la muestra verificamos la ip que toma nuestro equipo de escritorio conectado a la LAN.

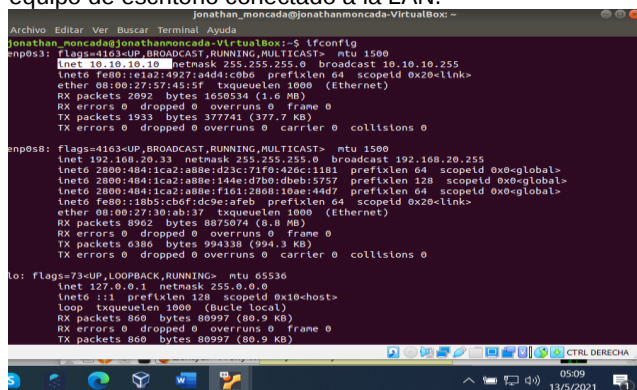


Fig. 56 validando ip en Desktop

Vamos a las opciones del navegador donde activamos el Proxy y lo configuramos con los datos de nuestro Proxy.

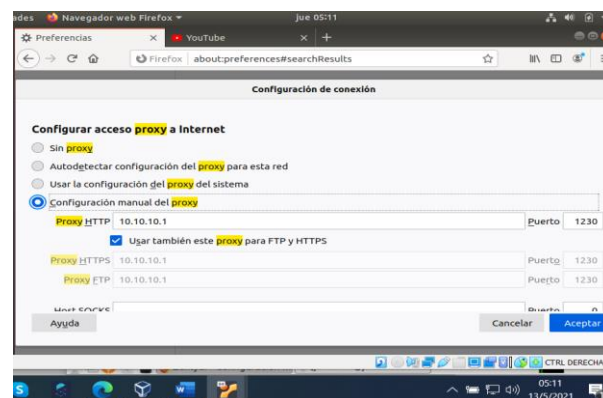


Fig. 57 activando proxy en Desktop

Posterior a eso realizamos la prueba de conexión.

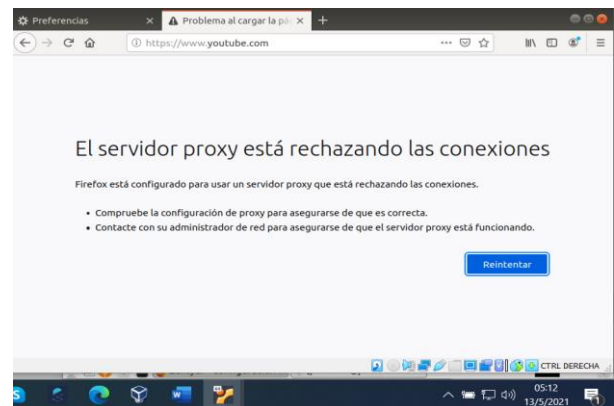


Fig. 58 1er prueba de conexión

Para confirmar el comportamiento del Proxy activamos el paso de tráfico desde el Proxy



Fig. 59 Editar regla de acceso

Luego del cambio realizado en el Proxy podemos comprobar el estado de conexión en el equipo con ubuntu Desktop.

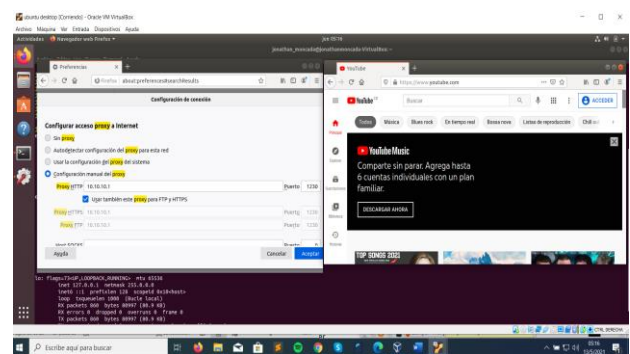


Fig. 60 2da prueba de conexión

3.2.1 Configuración de red

Tabla 1 Configuración de red Proxy no transparente

Zentyal	
Eth0	192.168.20.32/24
Eth1	10.10.10.1/24
Desktop	
Eth0	10.10.10.10/24
Eth1	192.168.20.33/24

3.3 CORTAFUEGOS

Instalación del componente Firewall a través de la consola web de administración de zentyal.

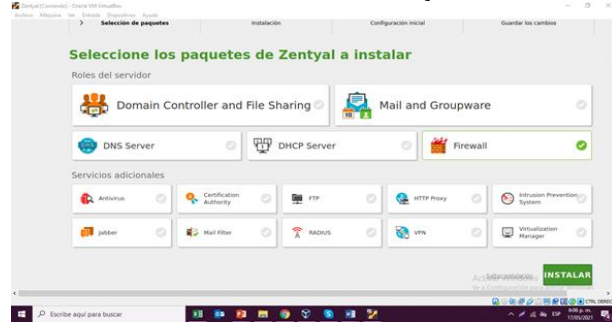


Fig. 61 Instalación del paquete de firewall

Al solicitar la instalación del paquete de firewall se instala también las configuraciones de red

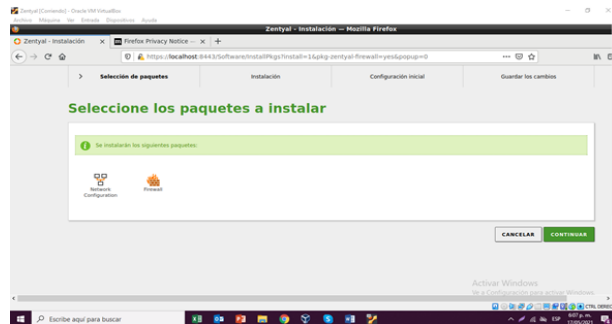


Fig. 62 Selección de paquetes

Se verifica que la instalación fue completada exitosamente

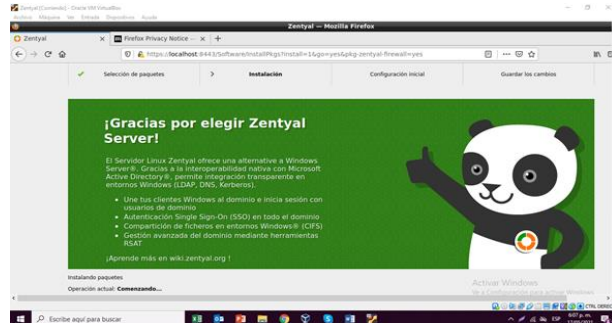


Fig. 63 Instalación completa

Se evidencia en la consola web el paquete firewall instalado, se inician configuraciones

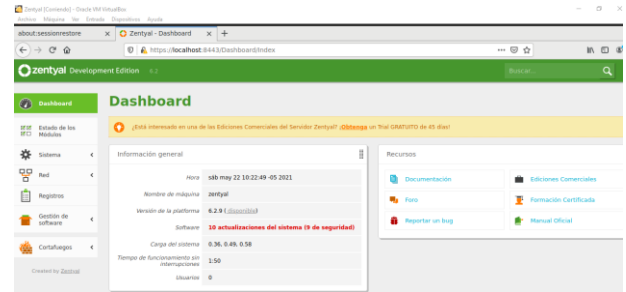


Fig. 64 Paquete firewall instalado

Configuración interfaces de red

eth0-LAN
192.168.0.122
255.255.255.0

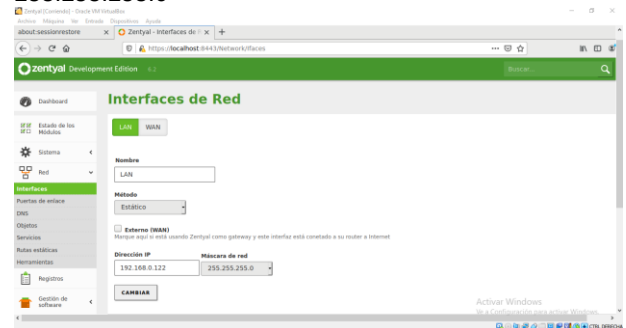


Fig. 65 configuración red LAN

eth1-WAN
192.168.1.200
255.255.255.0

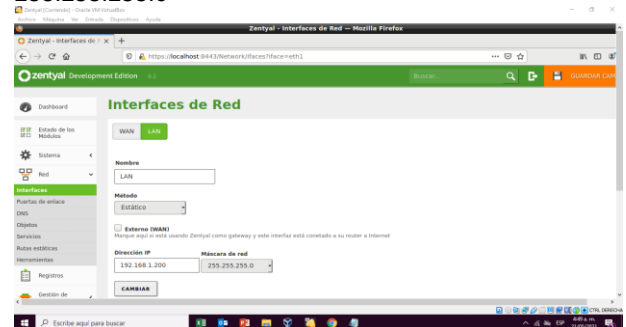


Fig. 66 configuración red WAN

Puerta de enlace
gateway: 192.168.0.1

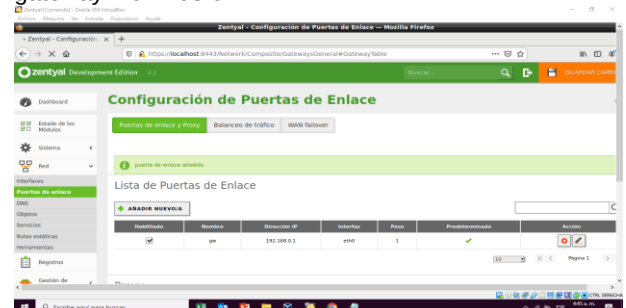


Fig. 67 configuración gateway

Configuración DNS

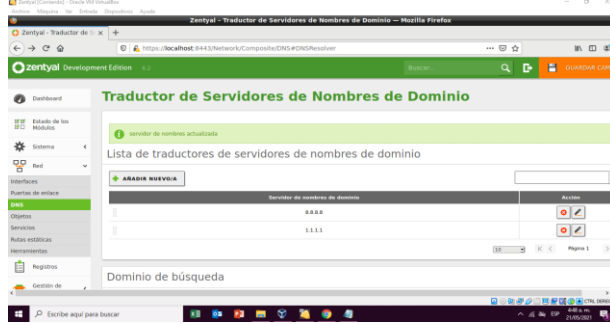


Fig. 68

3.4 FILE SERVER Y PRINT SERVER Configuración módulos

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

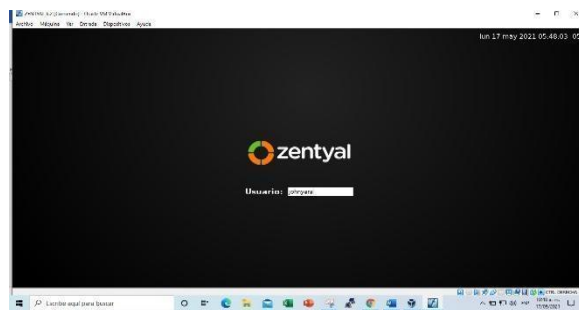


Fig. 68 Ingreso al programa Zentyal

Sí no están instalados los seleccionamos y continuamos.

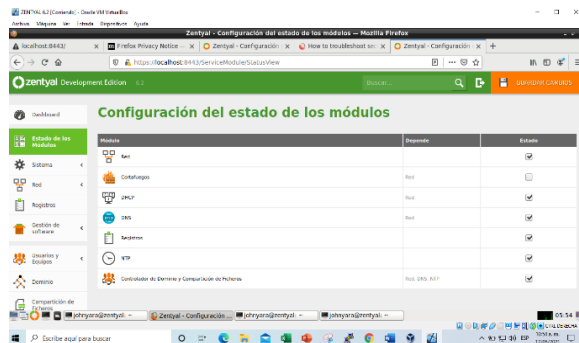


Fig. 69 Panel de control para la instalación de paquetes.

Es posible también actualizarlos si ya se encuentran instalados.

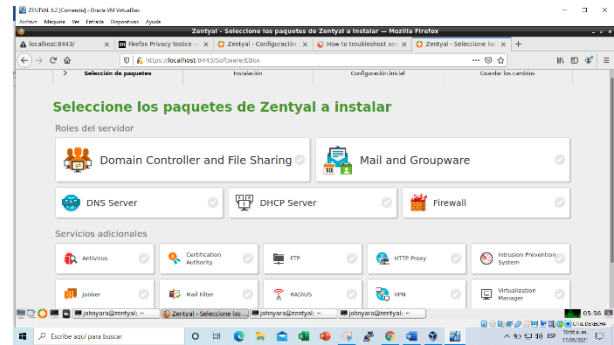


Fig. 70 Verificación de componentes de Zentyal.

Los servicios como el controlador de dominio permiten 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.

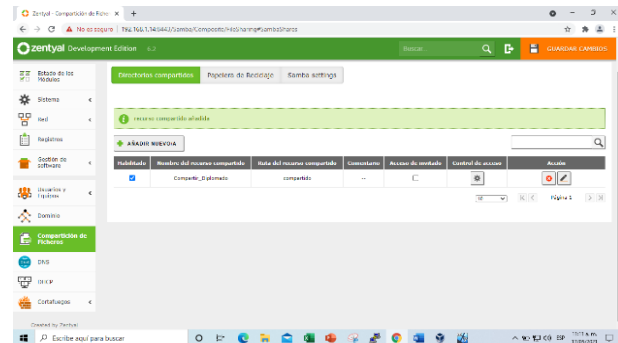


Fig. 71 Confirmación de aplicación de cambios.

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

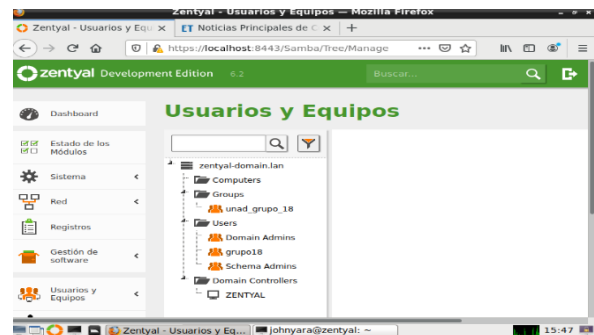


Fig. 72 Usuarios y Equipos

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



Fig. 73 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 habilita la opción. En este caso se crea el fichero compartido_linux.

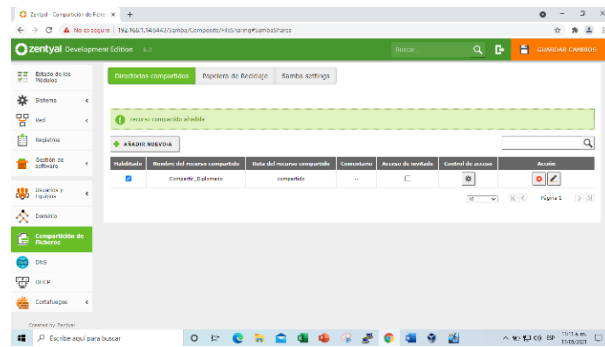


Fig. 74 Carpeta compartida en el servidor

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

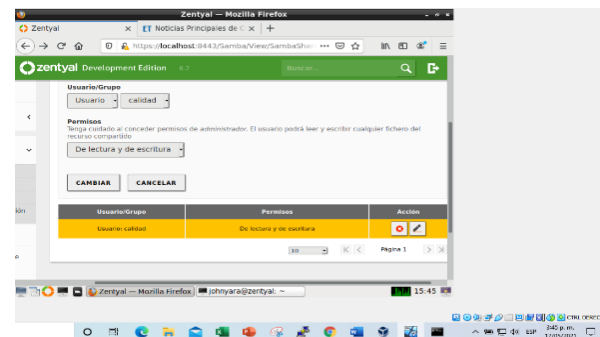


Fig. 75 Control de acceso a carpeta compartida.

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

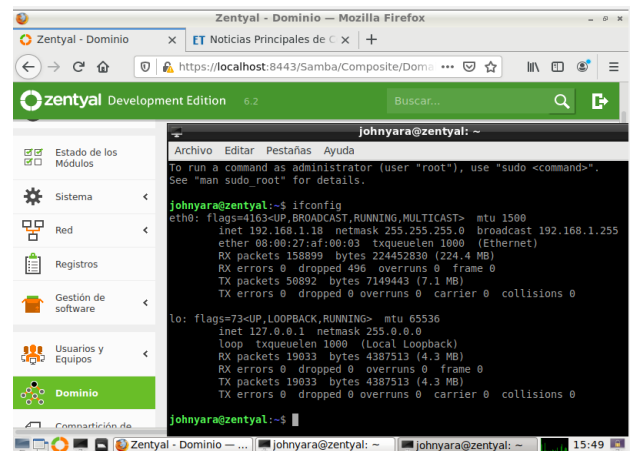


Fig. 76 Dirección IP de servidor.

Ahora desde un equipo con Windows 10 el cual se encuentra 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. \\192.168.1.18, luego conectamos con usuario creados para recursos compartidos.

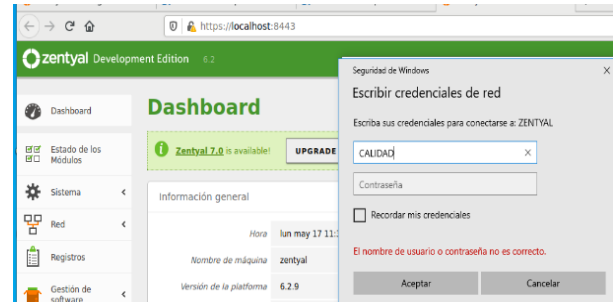


Fig. 77 Recurso compartido en la red

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 10 se crea carpeta para confirmar la correcta aplicación de seguridad en el directorio.

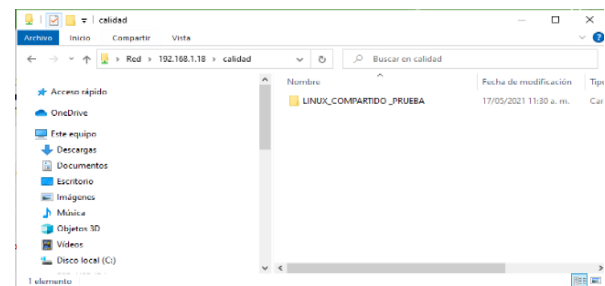


Fig. 78 Carpeta creada desde Win10.

Finalmente se ingresa a Ubuntu y se toma la Ip actual del sistema, luego desde Zentyal y con uso de SSH nos conectamos y podemos a conectarnos 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.

`https://192.168.1.18:631/admin`

Para la autenticación se usará el mismo usuario y contraseña con el que se accede al servidor.

Una vez iniciado 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.

3.5 VPN

Configuración servicio open vpn

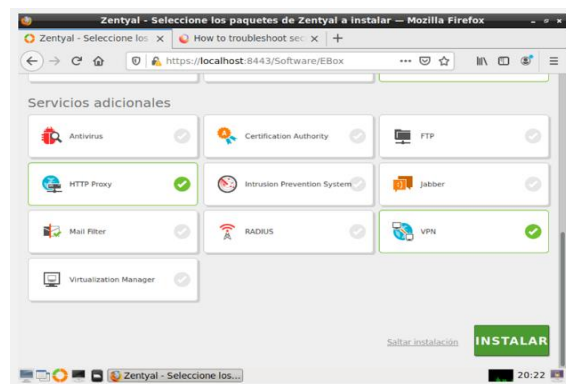


Fig. 79 Servicios a instalar

Cuando vamos a realizar la instalación del servicio OPEN VPN, seleccionamos el servicio VPN.

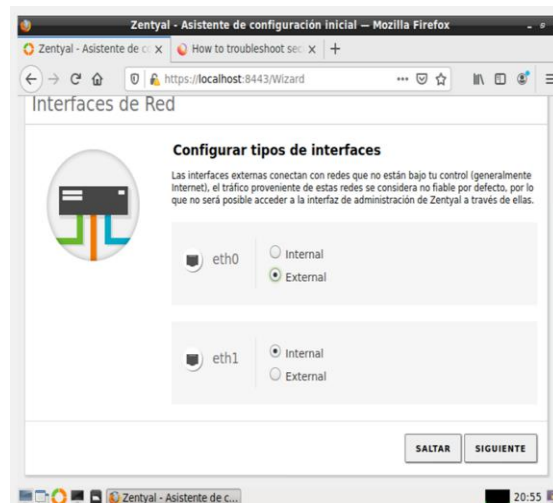


Fig. 80 interfaz de red

Posteriormente se configuran las interfaces de red, dejando una para red interna en modo estatico y la otra configurada como DHCP para recibir la conexión externa de internet.

Esta parte es muy importante ya que de aquí tomaremos la dirección ip que será la conexión de los certificados que se descarguen para los clientes externos que hagan uso de la VPN a través del servicio OPEN VPN.

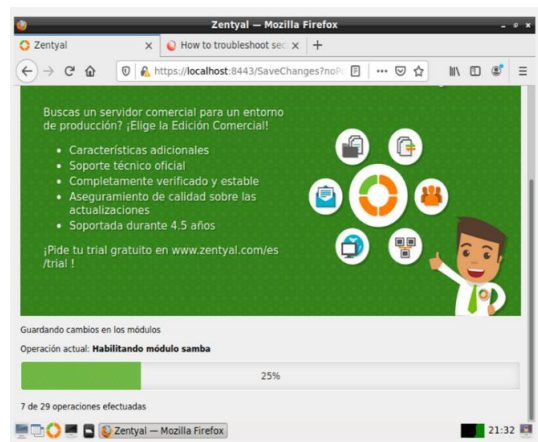


Fig. 81 proceso de instalación del servicio

Luego de revisar los servicios a instalar y haber solicitado la instalación del servicio VPN, debemos esperar a que el servidor realice el respectivo proceso y nos notifique la configuración exitosa.



Fig. 82 notificaciones de la instalación del servicio

Cuando los servicios se instalan correctamente, el servidor nos arroja una ventana de notificación.

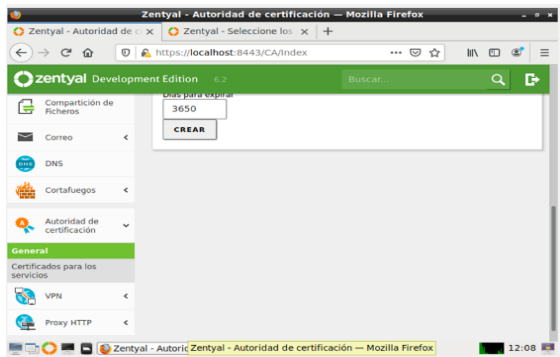


Fig. 83 Primer uso del servicio

Se direcciona a la parte izquierda y se verifica que estén los servicios de prerequisite para usar el servicio VPN, en total los tres servicios que deben estar activos son: Cortafuegos, autoridad de certificación y VPN.

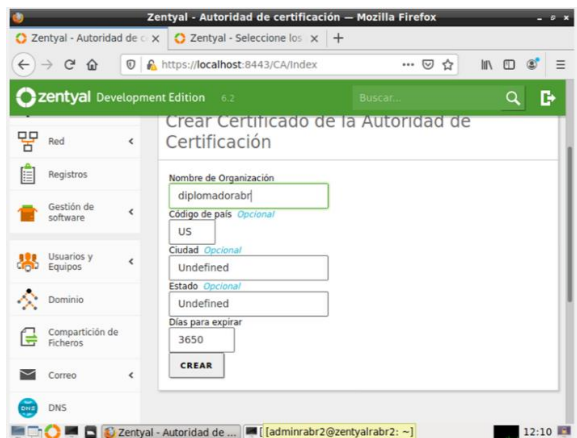


Fig. 84 Primer uso del servicio

Lo primero que debemos realizar es la creación de los certificados que generarán los archivos de conexión entre el servidor, el cliente y los servicios VPN.

El primer certificado que va para la aplicación zentyal se denominó "diplomadorabr" denotando las

letras iniciales del autor del proyecto, se dejaron por defecto los 3650 días para la expiración del certificado.

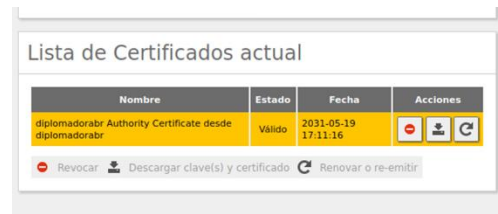


Fig. 85 Primer uso del servicio

Se verifica que el certificado haya quedado configurado correctamente.

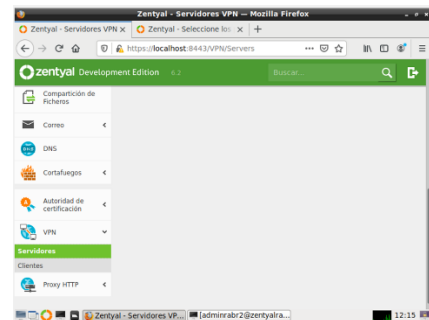


Fig. 86 creación del servidor

Luego de crear el certificado inicial, se procede a la creación del servidor, se debe seleccionar la opción VPN y luego servidores.

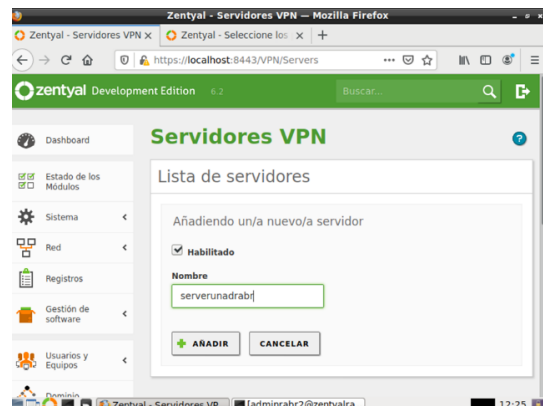


Fig. 87 datos básicos del servidor

Se procede a la creación del servidor VPN dentro del servicio open vpn y se nombre "serverunadrvpn" mencionado por las iniciales del autor de la explicación de este punto.

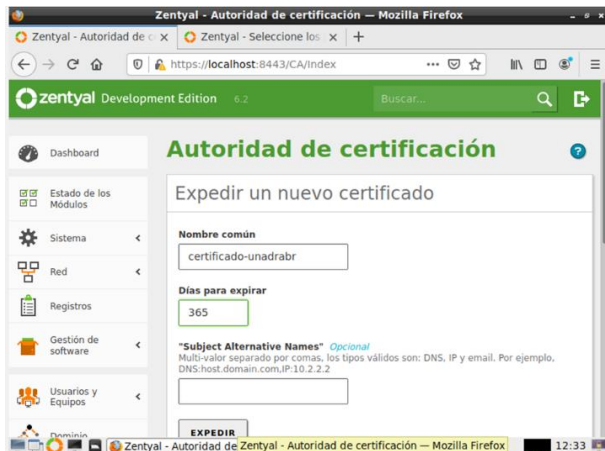


Fig. 88 certificado del servidor

Se genera el certificado del servidor VPN, este certificado es el que se podrá configurar para posteriormente descargar los certificados de conexión.

A diferencia del certificado anterior, este tiene un tiempo de expiración de 365 días.

Lista de Certificados actual

Nombre	Estado	Fecha	Acciones
diplomadorabr Authority Certificate desde diplomadorabr	Válido	2031-05-19 17:11:16	  
vpn-serverunabr.vpn	Válido	2031-05-19 17:11:16	  
certificado-serverunabr	Válido	2022-05-21 12:35:08	  

Revocar Descargar clave(s) y certificado Renovar o re-emitar

Fig. 89 validación de certificados

Se realiza la verificación de los certificados, para llegar a esa verificación se debe seguir la opción de autoridad de certificación y observar cuales son los certificados disponibles y activos en ese momento.

Lista de servidores

ANADIR NUEVO/A

Habilitado	Nombre	Configuración	Redes anunciadas	Descargar paquete de configuración de cliente	Acción
☒	serverunabr.vpn				

10 |< |> |Página 1

Fig. 90 listado de servidores

En esta opción se realiza la verificación de los servidores VPN disponibles, en este caso se evidencia que el servidor denominado "serverunabr" está listo para su proceso de configuración.

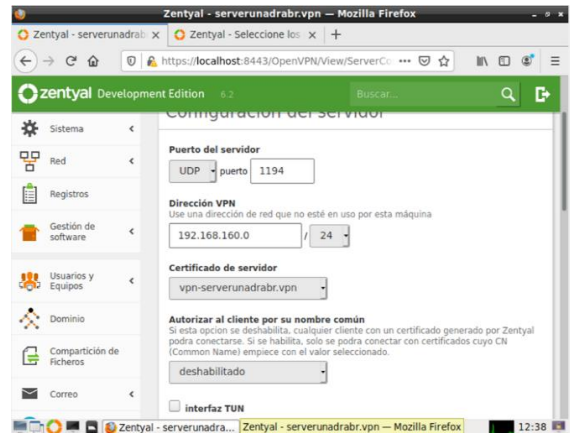


Fig. 91 listado de servidores

Se debe ingresar a la opción de configuración del servidor y se evidencia el puerto UDP 1194 que es el puerto por el que se realiza conexión con el cliente, la dirección ip se deja por defecto la que nos arrojó el servidor.

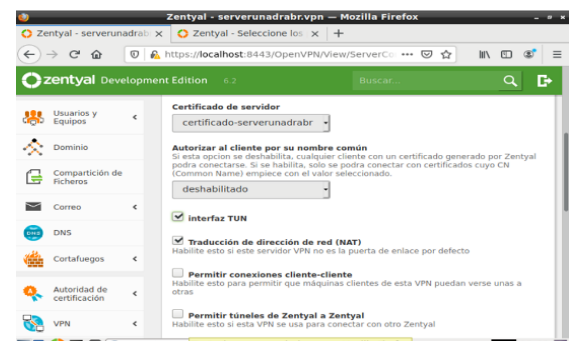


Fig. 92 Listado de servidores

Se realiza la activación de la interfaz TUN y las demás opciones se dejan por defecto.

En esta misma opción nos aparece.

Zentyl - Servicios - Mozilla Firefox

Zentyl - Servicios

Zentyl - Seleccione los : +

↶

↷

🏠

🔒

https://localhost:8443/Network/View/Service?li...

⋮

🔍

🏠

🔖

👤

☰

zentyl

Development Edition 6.2

Buscar...

🔍

🔗

Interfaz

Puertas de enlace

DNS

Objetos

Servicios

Rutas estáticas

Herramientas

📁

Registros

📁

Gestión de software

◀

👤

Usuarios y Equipos

◀

🌐

Dominio

Cualquier ICMP	Cualquier paquete ICMP			
Cualquier TCP	Cualquier puerto TCP			
Cualquier UDP	Cualquier puerto UDP			
Correo Entrante	Protocolos POP, IMAP y SIEVE			
Cualquiera	Cualquier protocolo y puerto			
DNS	Servicio de Nombres de Dominio			
Envío de Correo	Correo saliente (Protocolo de envío)			
HTTP	Protocolo de Transporte de hipertexto			
HTTPS	Protocolo de Transporte de hipertexto sobre SSL			
NTP	Network Time Protocol			

Fig. 93 listado de servidores

Se selecciona la opción RED, ubicada en la parte izquierda y luego se selecciona la opción de servicios

para confirmar que todos los servicios de red se encuentren arriba.



Fig. 94 listado de servidores

Se selecciona la opción “cortafuegos” ubicada en la parte izquierda y se procede a configurar el servicio de firewall que habilita el paso de tráfico del servicio OPEN VPN.

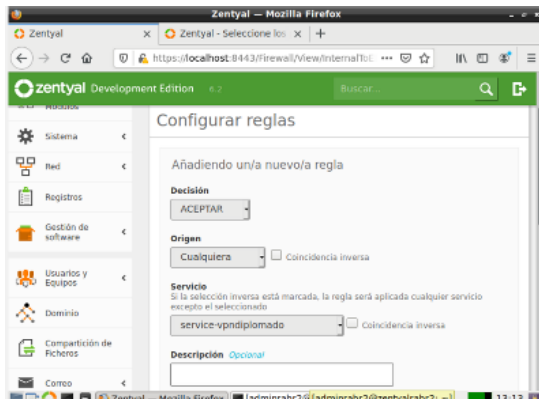


Fig. 95 Reglas de firewall

Se crea la regla de firewall permitiendo que acepte el tráfico originado desde cualquier equipo que tenga un certificado.

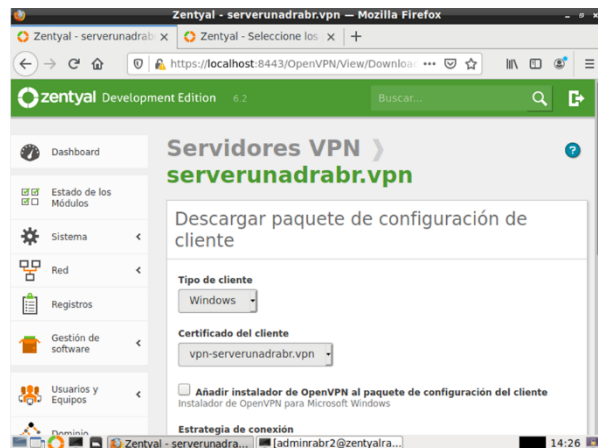


Fig. 96 Reglas de firewall

Posterior a esto, se selecciona la opción VPN, luego se escoge el servidor que se va a usar y se debe escoger la opción descargar paquete de configuración del cliente, en esta opción se selecciona el tipo de cliente que usará el servicio, sea Windows o Linux, se descarga y usando la herramienta OPEN VPN (instalándola en Windows o usando por defecto la que viene instalada en UBUNTU) se genera la conexión y uso del servicio VPN.

4 CONCLUSIONES

El sistema operativo Zentia cuenta con un grupo de herramientas que facilitan la puesta en marcha y administración de diferentes servicios que se pueden utilizar para satisfacer los requerimientos en relación a seguridad, conectividad, manejo de usuarios, permisos a ficheros o servicios que se puedan presentar en una infraestructura TIC, es importante resaltar que es una valiosa opción en el momento de que una compañía decida implementar software libre para la gestión y administración de sus redes informáticas.

Zentyal nos muestra ser un servidor sencillo de manipular, permitiéndonos administrar servicios de interés para la red de una empresa o incluso si lo queremos hacer de manera local. Y lo vimos con fácilmente con la aplicación sobre una maquina host de un Proxy no transparente, con el cual permitimos y denegamos el paso del tráfico con gran facilidad.

Zentyal permite el uso de herramientas para conexiones privadas y seguras como Open Vpn la cual permite que pequeñas y medianas empresas puedan acceder a estos servicios a un coste menor de lo que supone un software basado en herramientas que no son libres, su interfaz es muy amigable y permite usos como por ejemplo direccionar el tráfico para que sea administrado por medio de estas conexiones brindando mayor seguridad a la compañía. esta herramienta es de fácil uso tanto en la administración como en sus clientes dado que cuenta con su respectivo instalador para windows y viene instalado por defecto en las versiones posteriores de Ubuntu 18.02

5 REFERENCIAS

- [1] G. Obregón-Pulido, B. Castillo-Toledo and A. Loukianov, "A globally convergent estimator for n frequencies", IEEE Trans. On Aut. Control. Vol. 47. No 5. pp 857-863. May 2002.
- [2] H. Khalil, "Nonlinear Systems", 2nd. ed., Prentice Hall, NJ, pp. 50-56, 1996.
- [3] Francis. B. A. and W. M. Woynham, "The internal model principle of control theory", Automatica. Vol. 12. pp. 457-465. 1976.
- [4] Zentyal Community (22 de mayo de 2021) Servicio de redes privadas virtuales (VPN) con OpenVPN <https://doc.zentyal.org/6.2/es/vpn.html>.
- [5] Control Toolbox (6.0), User's Guide, The Math Works, 2001, pp. 2-10-2-35.
- [6] J. Jones. (2007, Febrero 6). Networks (2nd ed.) [En línea]. Disponible en: <http://www.atm.com>.

- [7] Instalación — Documentación de Zentyal 6.2. (s/f). Recuperado de Zentyal.org website: <https://doc.zentyal.org/6.2/es/installation.html>
- [8] Servicio de resolución de nombres de dominio (DNS) — Documentación de Zentyal 6.2. (s/f). Recuperado de Zentyal.org website: <https://doc.zentyal.org/6.2/es/dns.html>
- [9] Información sobre Zentyal 6.2 <https://zentyal.com/es/news/zentyal-6-2-announcement-2/>