

# INSTALACIÓN Y CONFIGURACIÓN DHCP SERVER, DNS SERVER Y CONTROLADOR DE DOMINIO, PROXY NO TRANSPARENTE, CORTAFUEGOS, FILE SERVER, PRINT SERVER Y VPN

Alexander Ibañez Casallas  
e-mail: aibanezc@unadvirtual.edu.co  
Giovanni Martínez  
e-mail: gmartinezfa@unadvirtual.edu.co  
Iván Parra González  
e-mail: iaparrag@unadvirtual.edu.co  
Jorge Jonathan Fique Camacho  
e-mail: jjfiquiec@unadvirtual.edu.co

**RESUMEN:** *Este artículo evidencia la instalación, configuración y puesta en marcha con GNU/Linux Zentyal Server conforme a las exigencias en los servicios de red en la Infraestructura IT para el proceso integral de migración y capacitación de la infraestructura tecnológica en la empresa Internacional Proveedores de Servicios de Internet ISP. Demuestra la implementación y ejecución detallada de los servicios de gestión de red DHCP Server, DNS Server, Controlador de Dominio, Proxy no transparente, Cortafuegos, File Server, Print Server y VPN.*

**PALABRAS CLAVE:** Zentyal Server, conectividad, DHCP, cortafuegos, File Server, Print Server, Proxy http.

## 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.

Este artículo exhibe la instalación, configuración y administración GNU/Linux Zentyal Server de alto rendimiento, seguridad y estabilidad acorde a las necesidades empresariales. Aborda los servicios de la red de computadores con bloqueos y permisos de acceso en las comunicaciones, la implementación se enfoca en una solución segura y en el resguardo de la información sensible con un controlador de dominio que administra las credenciales en el inicio de sesión y actúa con un filtro entre la conexión a internet, restricción de los servidores y la comunicación en la red verificando las conexiones de forma segura, aísla las diferentes redes con una zona perimetral segura que protege las consultas hacia internet con un proxy que asigna un certificado aceptado por el cliente para dar continuidad a la comunicación o una alerta de conexión insegura, redirige los puertos en los protocolos, instaura un conjunto de políticas de filtrado de tráfico y regula el uso de los otros puertos definidos en un cortafuego.

## 2. MARCO TEORICO

Zentyal Server Zentyal Server es una distribución de Linux tipo servidor código abierto, basado en Ubuntu que maneja una interfaz web por medio de Apache. Está

diseñado para administrar la infraestructura de red. Tiene 2 versiones: una de desarrollo que es gratuita para su uso, pero no se recomienda para implementar en producción, mientras que su versión comercial indica que son una alternativa a Windows server, permitiendo implementar una gran variedad de servicios como el acceso a internet, seguridad de la red, comunicaciones, dominio, entre otros.

Se desarrolló con el fin de solucionar los problemas de control y seguridad de las redes en pequeñas y medianas empresas y ser una alternativa más económica frente a Windows server, donde su licenciamiento se basa en costos de acceso al servidor.

La principal característica de Zentyal Server es su compatibilidad nativa con los protocolos de Microsoft® Exchange Server. Soporte para Microsoft Outlook® 2007, 2010. Compatibilidad nativa con Microsoft Active Directory® 2008, 2008R2, 2012. Email, calendarios, contactos.

### 2.1 GNU/LINUX ZENTIAL SERVER

El servidor de red Zentyal bajo una distribución GNU/Linux se basa en Ubuntu 18 para administrar los principales servicios de la red informática, controla el acceso a Internet brindando seguridad en las comunicaciones de red mediante el navegador web.

### 2.2. PROCESO DE INSTALACIÓN

GNU/Linux Zentyal se integra con módulos configurables actuando en la red, la fuente del instalador se aloja en su sitio web con el enlace de zentyal-6.2-development-amd64.iso. Al completar la descarga se define la configuración de la máquina virtual e inicia la instalación fijando la zona horaria y teclado.

Luego se asigna el nombre del servidor en la red local, la configuración del usuario, el proxy HTTP para acceder a la red, el cargador de arranque GRUB en el registro principal y la hora local del sistema.

Finalizada la instalación se acepta la advertencia del certificado autoafirmado en la accediendo al puerto 8443 en el navegador, así <https://127.0.0.1:8443/>

### 3. INSTALACION DE ZENTYAL SERVER

#### 3.1. REQUISITOS DE INSTALACION

A nivel de Hardware Zentyal puede funcionar bajo la arquitectura de x86 y x\_64, como requerimientos mínimos a nivel de memoria RAM de debe tener 1 Gb y un disco duro de 30 Gb y dos tarjetas de red.

#### 3.2. INSTALACION DE S.O. Ubuntu Server 20.04

Se crea un VM donde se instalará el S.O. Ubuntu Server 20.04.

Se selecciona el idioma en el cual se instalará el S.O.

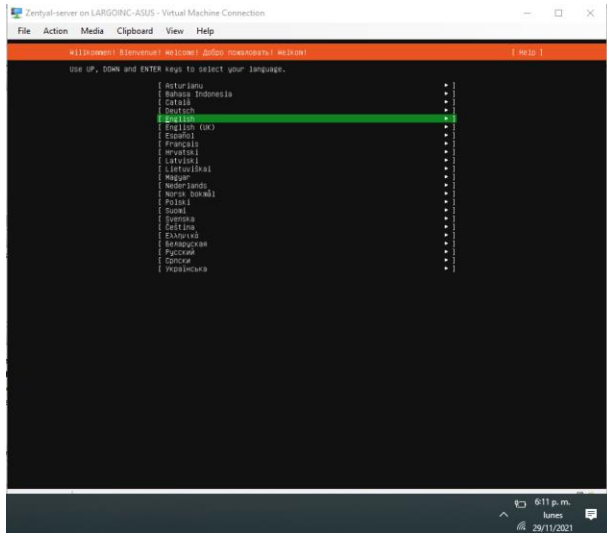


Imagen 1. Inicio de instalación del S.O.

En este paso se seleccionará el idioma del teclado o lo seleccionamos la detección de manera automática.

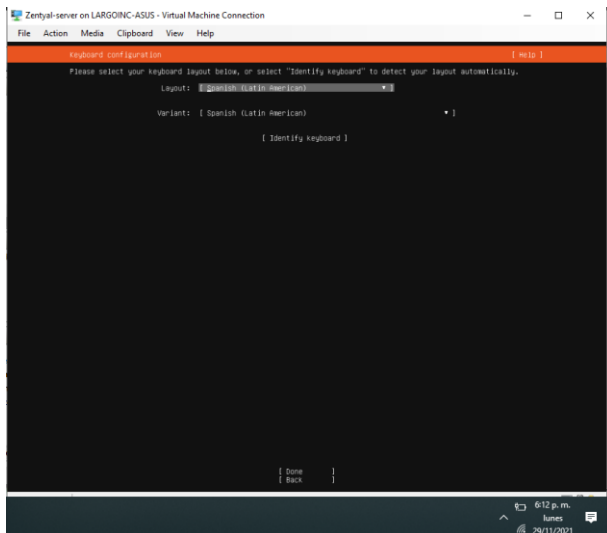


Imagen 2. Seleccionar Idioma.

Podemos seleccionar la configuración de la tarjeta de red tomando el direccionamiento IP automático o de manera estática.

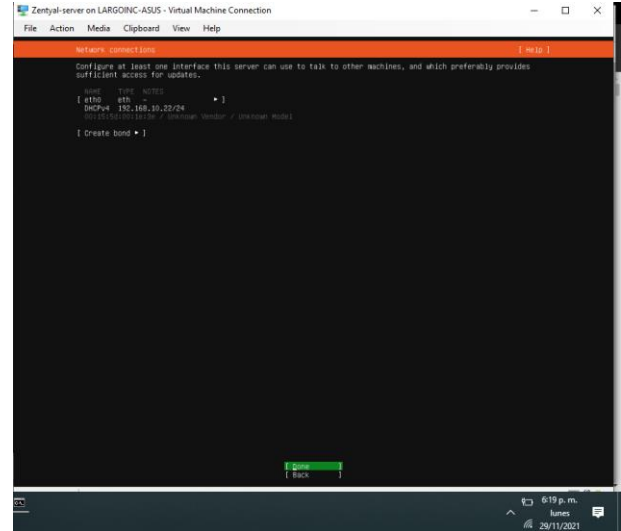


Imagen 3. Seleccionar IP.

Dejamos por defecto la URL donde podemos descargar una imagen espejo del S.O.

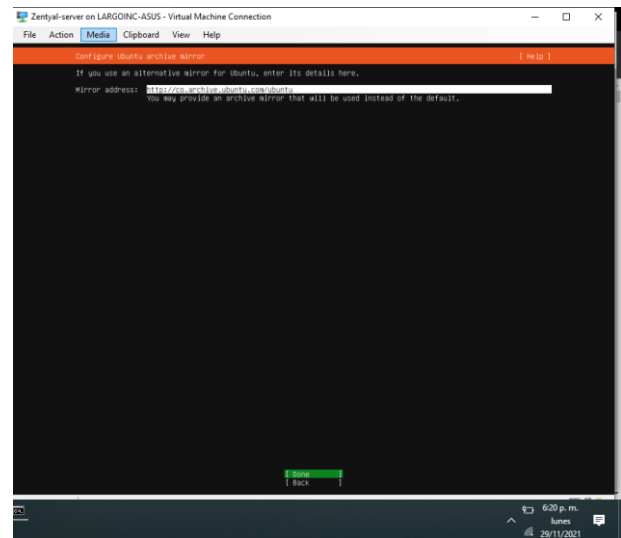


Imagen 4. URL de mirror del S.O.

Seleccionamos el disco en el cual se configuraran las particiones que se requiere para la instalación del S.O.

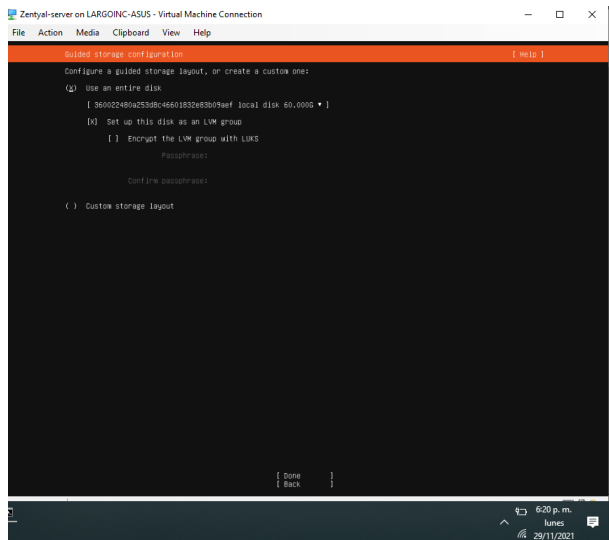


Imagen 5. Selección del disco de almacenamiento.

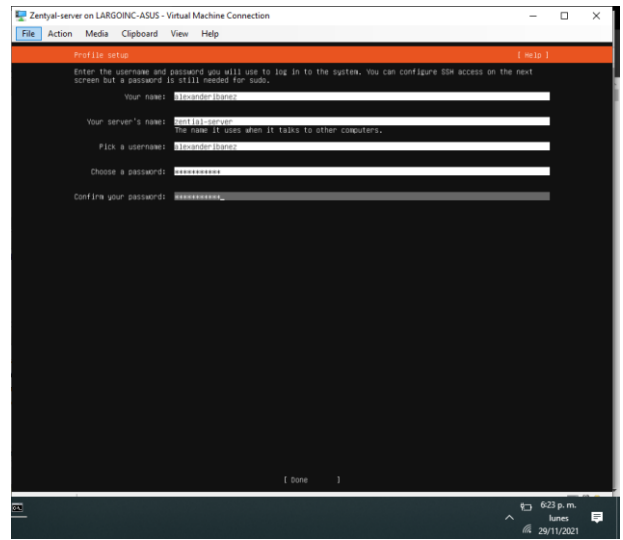


Imagen 7. Configuración del usuario root.

Confirmamos la configuración por defecto de las particiones de las unidades o las ajustamos de acuerdo con nuestras necesidades.

Validación del proceso de instalación del S.O. y posterior reinicio.

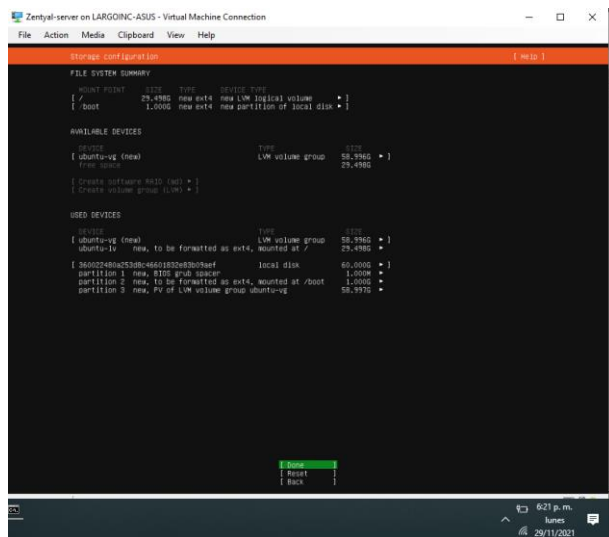


Imagen 6. Configuración de las particiones.

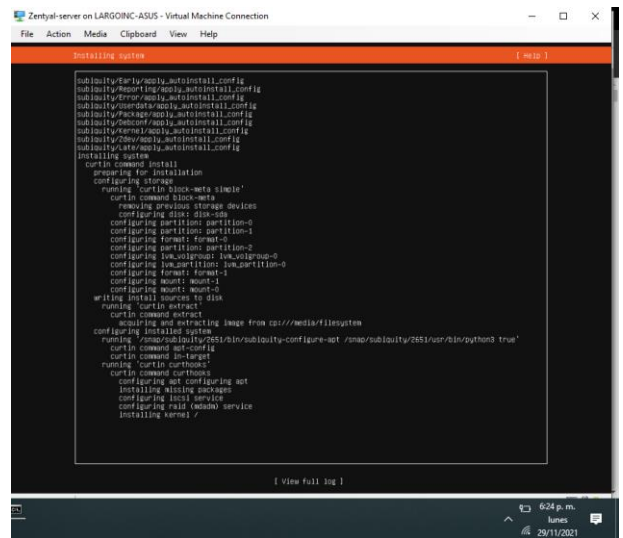


Imagen 8. Proceso de instalación.

Configuramos el nombre del usuario, nombre del servidor y la contraseña del usuario root o administrador.

Configuración y asignación de una IP estática en el servidor como buena práctica y mejor administración.

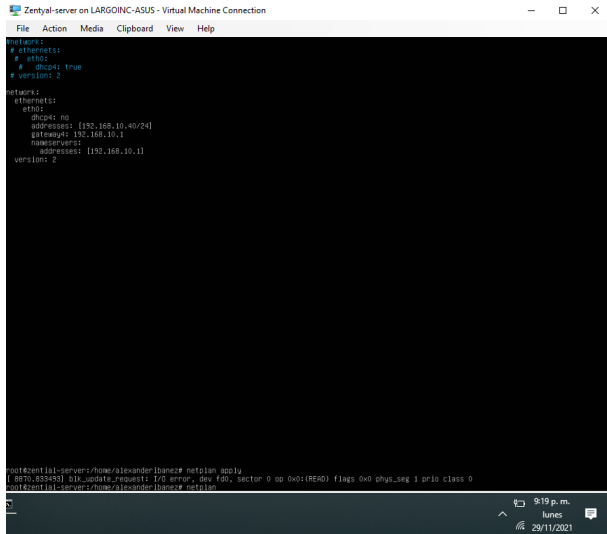


Imagen 9. Configuración de IP estática.

### 3.3. INSTALACION DE ZENTYAL

Procedemos a hacer la actualización del servidor ejecutando los comandos como modo root apt-get update y apt-get upgrade.

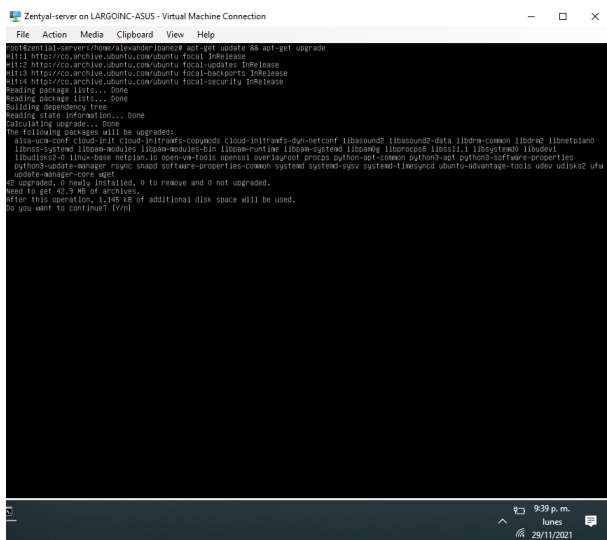


Imagen 10. Actualización del S.O.

Luego de tener actualizado el S.O. procedemos con la instalación de Zentyal descargando el script de instalación de la siguiente url: wget https://zentyal.com/zentyal\_installer.sh

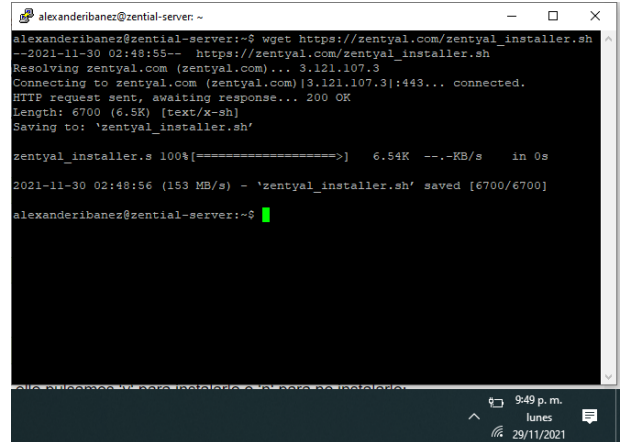


Imagen 11. Descarga del script de instalación.

Ahora procedemos a proporcionar permisos para la ejecución al script con el comando y ejecución del script para el proceso de instalación y confirmamos su instalación.

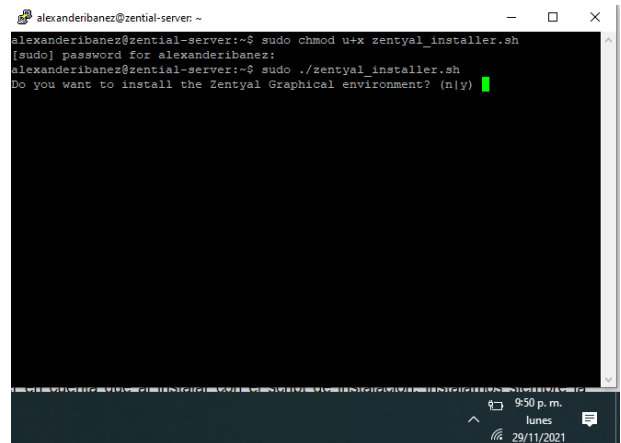


Imagen 12. Permisos y ejecución del script.

Luego de varios minutos se termina la instalación de forma satisfactoria donde nos indica la URL de ingreso a la plataforma de administración:

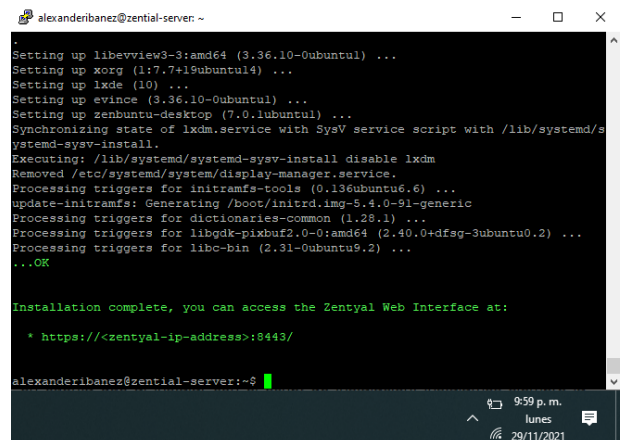


Imagen 13. Finalización de la Instalación.

Ingresamos a la URL para validar el ingreso donde introduciremos el usuario y contraseña root o administrador del S.O.

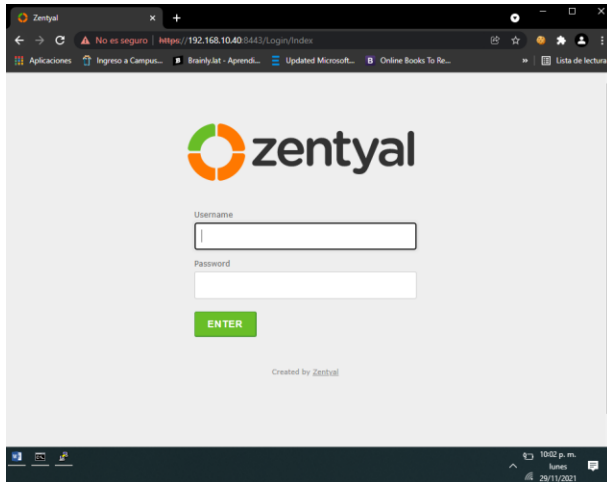


Imagen 14. Página principal del portal de acceso.

Luego de dar Continuar al asistente tendremos la siguiente pantalla donde seleccionaremos los servicios de DHCP Server, DNS Server y Controlador de Dominio.

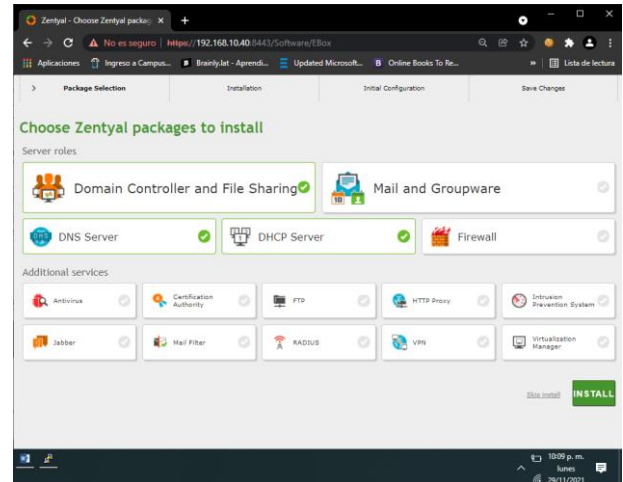


Imagen 16. Selección de los servicios.

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

Implementación y configuración detallada del acceso de una estación de trabajo GNU/Linux a través de un usuario y contraseña, así como también el registro de dicha estación en los servicios de Infraestructura IT de Zentyal.

Se inicia el proceso de instalación de los servicios que se requieren implementar en nuestro entorno.

Como prerequisite seleccionamos los siguientes servicios para poder instalar los servicios de DNS, DHCP y Controlador de Dominio.

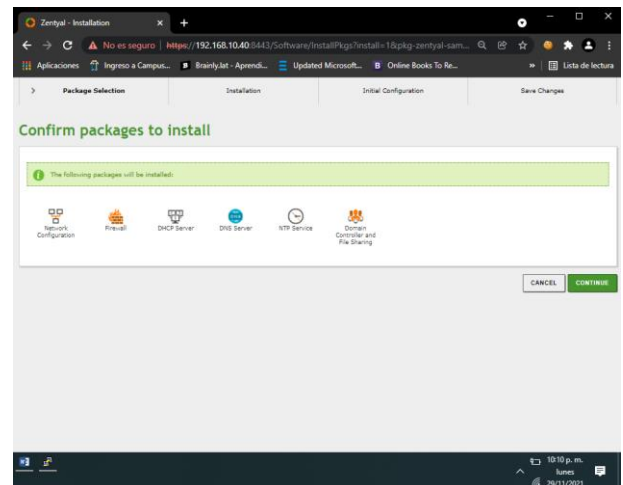


Imagen 17. Servicios prerequisites.

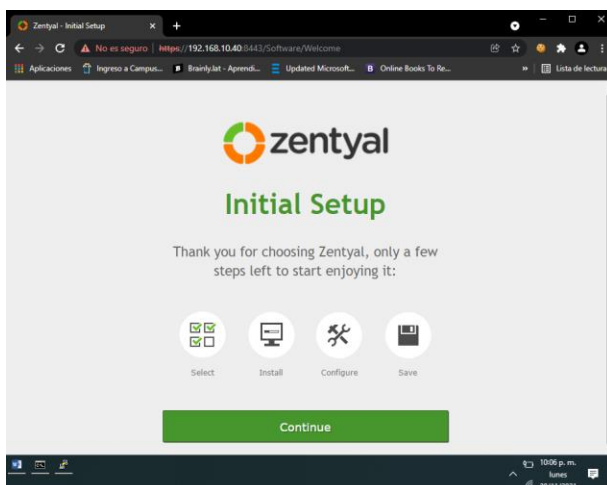


Imagen 15. Configuración Inicial.

Comienza el proceso de instalación de los diferentes paquetes requeridos para tener los servicios requeridos activos.

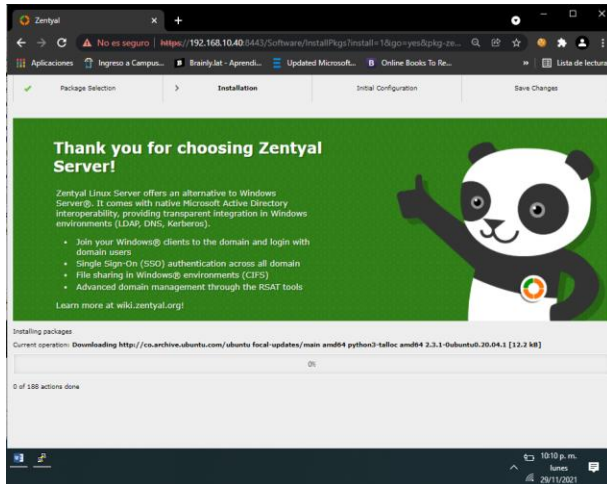


Imagen 18. Proceso de instalación.

Se tiene el proceso de instalación correcto y podemos ingresar al dashboard donde se monitorearán los servicios instalados.

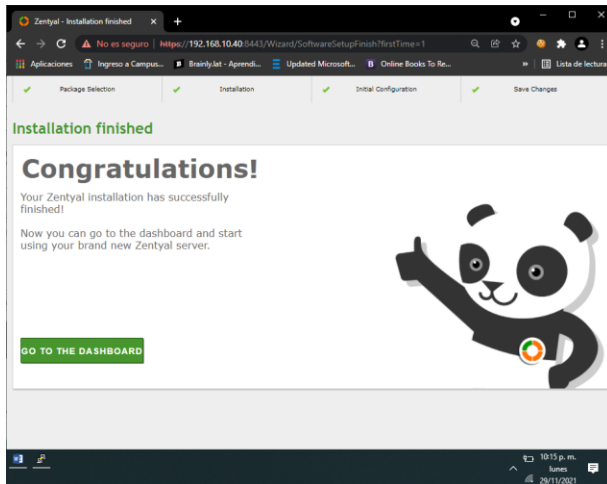


Imagen 19. Finalización de la instalación.

Como primer paso vamos al Module Status y seleccionamos cada uno de los servicios que instalamos para así poder subir los servicios y proceder a su configuración,

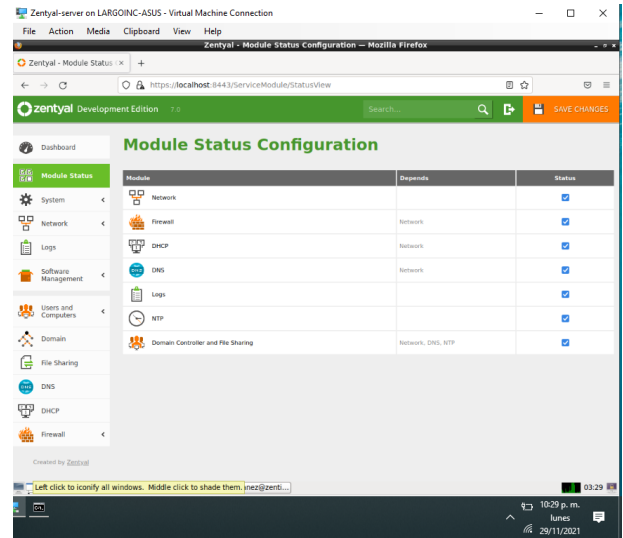


Imagen 20. Selección de servicios.

Desde el dashboard podemos monitorear y observar el estado de los servicios y su reinicio, para nuestro caso todos están Running.

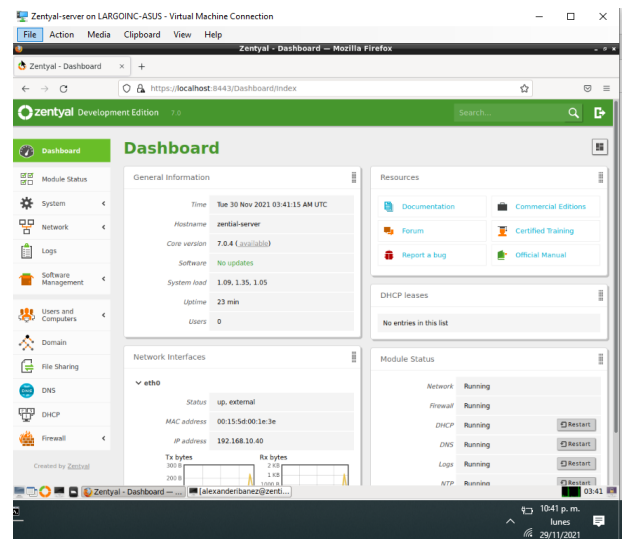


Imagen 21. Estatus de los servicios.

#### 4.1. DHCP Server

Se valida la IP definida en el servidor el cual se tiene para que los equipos puedan acceder a los servicios que para este caso es el DHCP.

Desde el dashboard podemos evidenciar la asignación de la 192.168.10.50 al equipo cliente alexanderibanez-virtual-machine por medio del servicio de DHCP.

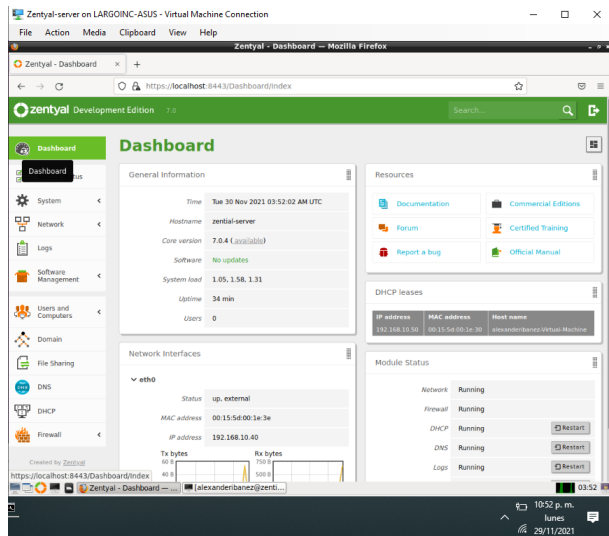


Imagen 22. Asignación de IP por DHCP.

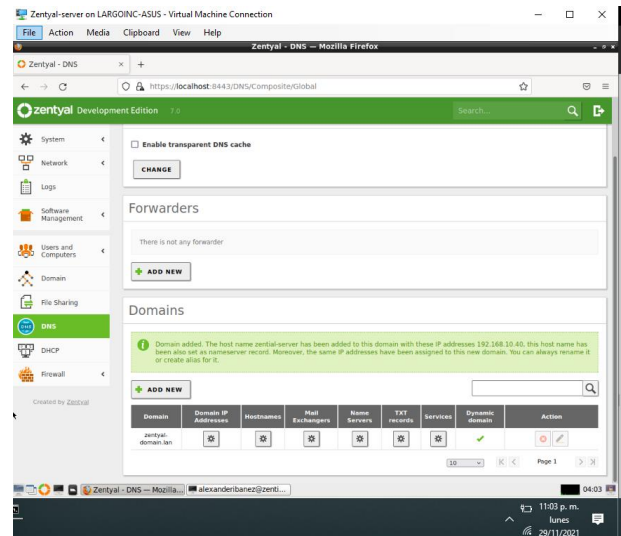


Imagen 24. Validación servicio DNS

En la siguiente imagen podemos ver que el equipo cliente toma la IP por medio del servidor DHCP.

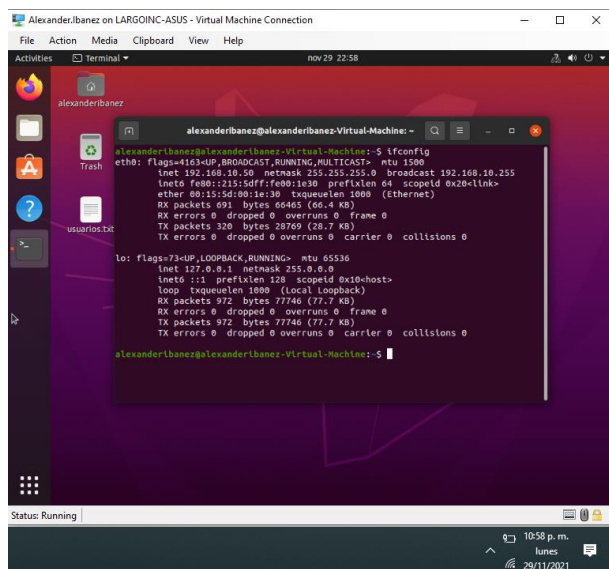


Imagen 23. Equipo Cliente.

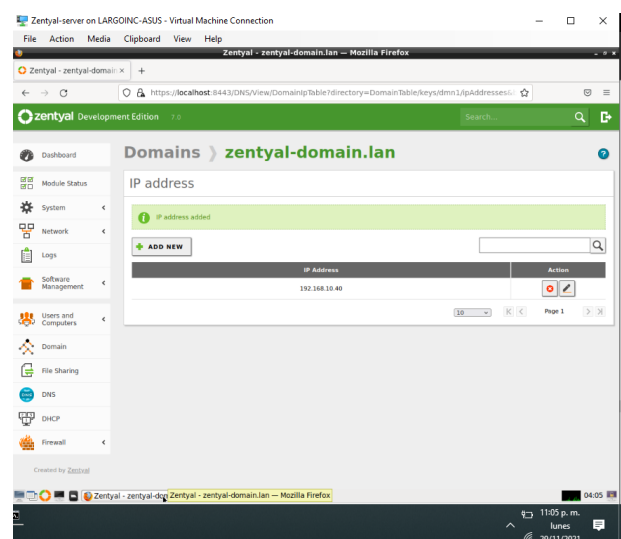


Imagen 25. IP asignada al servicio DNS.

## 4.2. DNS server

Se ingresa al módulo de DNS donde se configura el dominio y la IP que se le asignara a los equipos de la red, también la puerta de enlace para salida a internet cuando se requiera.



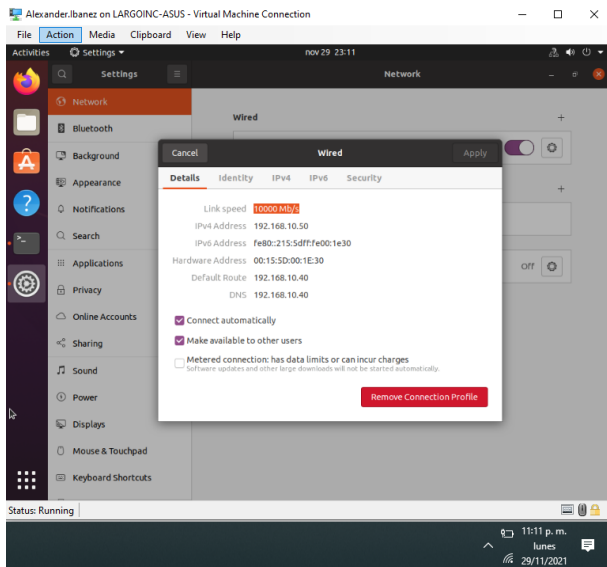


Imagen 26. Validación desde el equipo cliente.

### 4.3. Controlador de dominio

A nivel de servicio de Controlador de dominio se valida el servicio, el NetBios del servidor y del dominio, y la letra donde se almacena la base de datos pertinente.

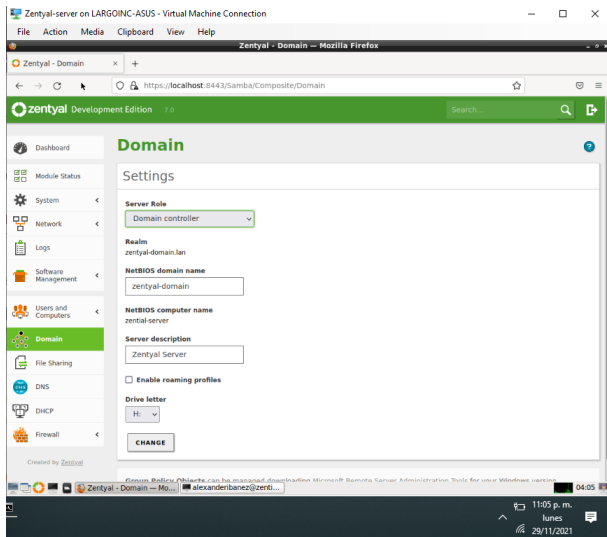


Imagen 27. Configuración del controlador del dominio.

Ingresamos al módulo de Users and Computers donde tenemos el árbol de la estructura base para poder crear tanto usuarios como grupos y visualizamos los objetos miembros del dominio.

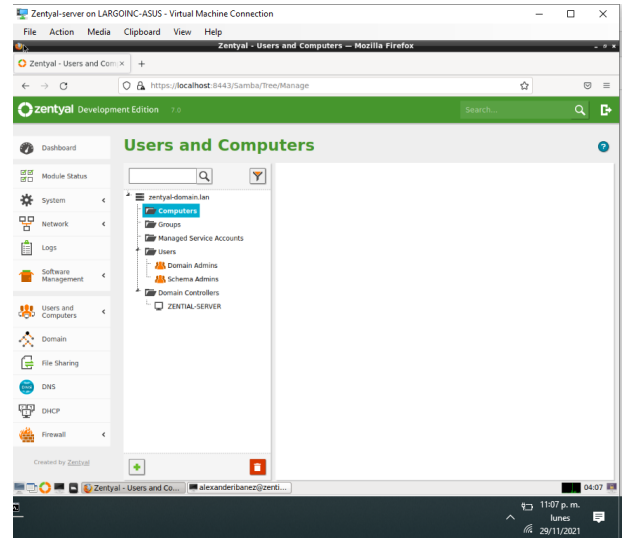


Imagen 28. Estructura del dominio.

Tenemos también la configuración de los CN y DN para permitir a terceros conectarse al LDAP y poder hacer consultas y modificaciones.

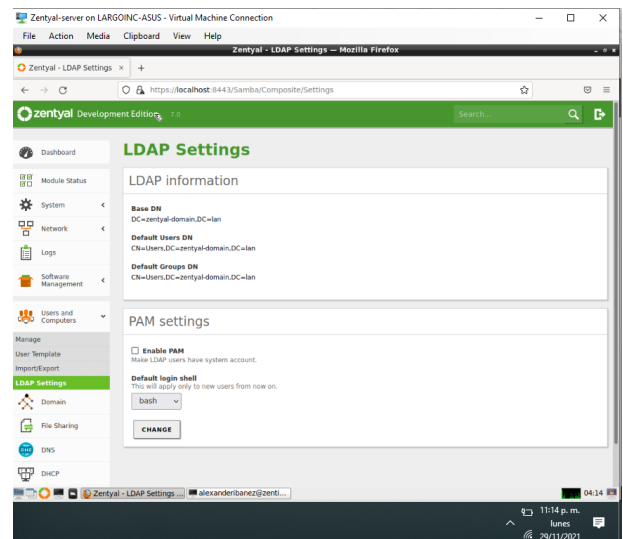


Imagen 29. Configuración del LDAP.

## 5. TEMÁTICA 2: PROXY NO TRANSPARENTE

El proxy http nos permite filtrar paquetes http y es usado normalmente para el control de la navegación en páginas web de internet.

Para realizar la implementación y configuración del control del acceso de estaciones de trabajo a los servicios de conectividad a Internet desde Zentyal a través de un proxy que filtra la salida por medio del



puerto 1230, se debe primero realizar la instalación del servicio como mínimo de firewall y proxy

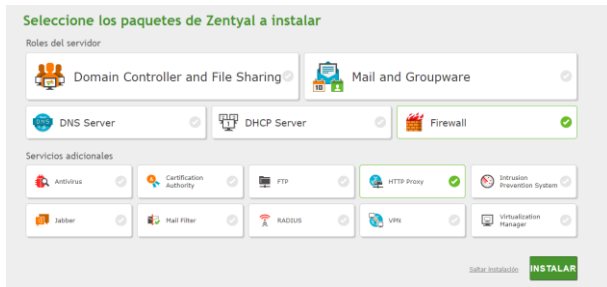


Imagen 30. Instalación de componentes Firewall y Proxy

Una vez instalado se debe habilitar el servicio para poder ser usado

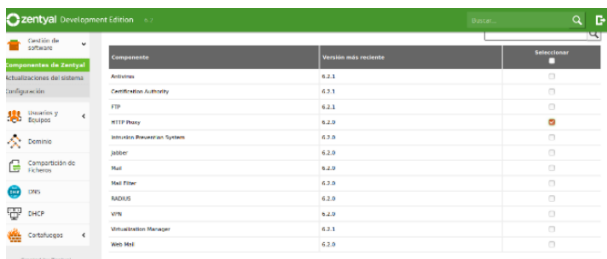


Imagen 31. Activación del proxy Http  
En configuración general configuramos el puerto que deseamos en nuestro caso 1230



Imagen 32. Cambio de puerto del proxy

Una vez activado ya podemos iniciar con la creación del perfil y el control de acceso, normalmente los proxys se usan de manera restrictiva, cerrando toda la navegación y permitiendo las páginas o dominios que deseamos que los usuarios puedan navegar



Imagen 33. Configuración de filtro web

Los proxys http pueden controlar todo el tráfico mediante el puerto que se le asigmo, por lo que debe ser configurado en el navegador web para que funcione el filtrado, a esto se le llama proxy no transparente, ya que el administrador debe encargarse de crear políticas de aplicación y restricción del cambio de este por medio del directorio activo.

Para el caso de proxy transparente se usa los segmentos de red y asignación de direcciones Mac para aplicar estas restricciones

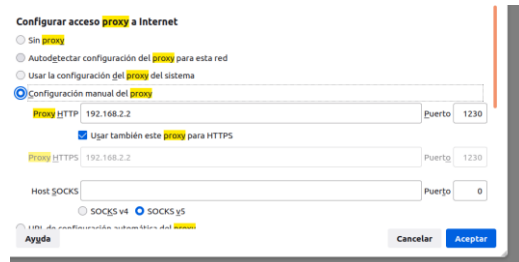


Imagen 34. Configuración de navegador

En este momento ya el proxy funciona correctamente y en caso de denegar nos mostrara un mensaje que informa al usuario que el proxy denegó la conexión y en caso de permitir simplemente se abre la pagina web

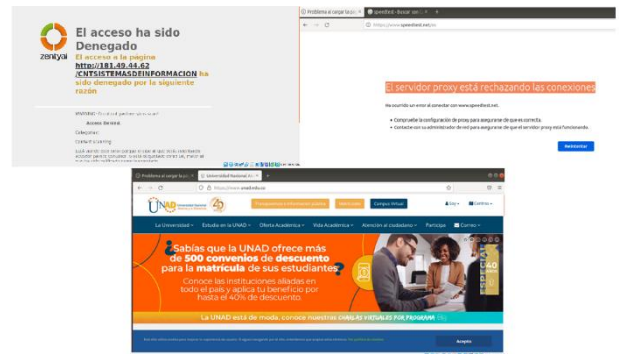


Imagen 35. Proxy en funcionamiento

Con el proxy también podemos controlar el ancho de banda que usa cada usuario, gracias a que todas las peticiones deben pasar por el puerto anteriormente configurado, para poder controlar el ancho de banda se puede configurar por estación de trabajo o por segmento de red, en este caso se configuro por segmento de red, ya que es mucho más sencillo administrar y se crean

menos objetos, para esto es necesario crear un objeto con el rango de direcciones Ip y luego de esto se crea la política de reducción de velocidad

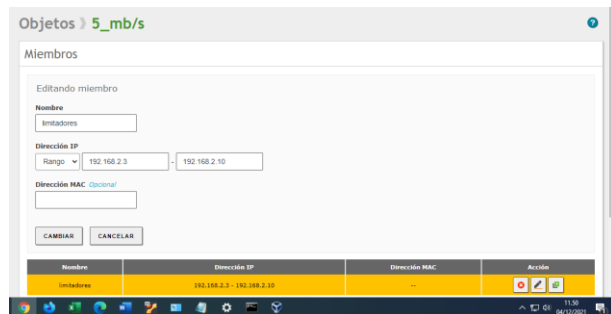


Imagen 36. Rango de red

Para la restricción de velocidad o control Zentyal usa un algoritmo en donde se permite el uso del ancho de banda total de la red hasta un tope de Megabytes descargados, luego de superar este umbral se procede a reducir la velocidad de transferencia a la indicada en la regla, en este caso se crea un perfil de 3 mb/s de penalización después de sobrepasar el ancho de banda de 200 mb. De esta manera evitamos que la red de internet y en general se sature por excesos de tráfico por algún usuario que realice una descarga de un archivo muy grande, por un tiempo extendido.



Imagen 37. Restricción de velocidad Funcionando

## 6. TEMÁTICA 3: CORTAFUEGOS

Implementación y configuración detallada para la restricción de la apertura de sitios o portales Web de entretenimiento y redes sociales, evidenciando las reglas y políticas creadas. La validación del funcionamiento del cortafuego aplicando las restricciones solicitadas, se hará desde una estación de trabajo GNU/Linux.

Una vez la configuración del DHCP y DNS han sido realizadas y comprobadas, con el fin de establecer políticas en el cortafuegos es necesario realizar su instalación, para en la configuración inicial del Zentyal puede realizarse su instalación, o en caso contrario desde Gestión de Software.



Figura 38. Instalación componente Firewall

Con el componente instalado, la configuración consiste en la creación de un servicio, un objeto y las reglas correspondientes.

### 6.1 CREACIÓN DE SERVICIO

Un servicio permite delimitar a nivel de protocolo y puerto los elementos que serán tratados, para el caso particular se crea uno cuyo propósito sea analizar el tráfico TCP/UDP bajo los puertos 80 y 443, correspondientes a los servicios Web, para esto desde el menú *Red* bajo *Servicios* se crea este:



Figura 39. Creación de servicio

Una vez ha sido creado se agregan los dos elementos mencionados correspondientes al protocolo y puertos:



Figura 40. Adición de servicio

### CREACIÓN DE OBJETO

El objeto nos va a permitir reconocer a quién se va a gestionar en el cortafuegos, en este caso se creará uno donde se defina el rango de IP usadas por Twitter que será el sitio que será bloqueado, pruebas realizadas indican que esta página responde a la red 104.244.42.x, por lo que el objeto tendrá como característica este rango de IP:



Figura 41. Objeto para gestionar

### CREACIÓN DE REGLA

Puesto que, por medio del servicio se reconoce qué se va a gestionar, y con el objeto a quién se gestionará, la regla nos permite determinar qué se va a realizar entre estos dos elementos, para ello se debe reconocer los siguientes elementos:

**Decisión:** Indica qué se realizará con los paquetes que cumplan las características de la regla, las opciones son: Permitir, Denegar o Registrar. En el caso actual se usará Denegar puesto que se pretende el bloqueo de conexiones.

**Origen:** Determinar desde qué punto origen se ejecutará la operación por parte del cortafuegos, se puede determinar una IP en particular o un objeto, para esta actividad se dejará como Cualquiera, de esta forma cualquier origen ejecutará la regla.

**Destino:** Determina a qué punto final va dirigida la comunicación, en este caso se hará uso del objeto previamente creado para que tenga en cuenta las IP relacionadas a Twitter.

**Servicio:** Cuando la regla se aplica, determina a qué protocolo/puerto aplicará, y se usará el servicio creado previamente.

**Descripción:** Indicación breve sobre el contenido de la regla para propósitos de reconocimiento.

Con esta configuración la regla tendrá estas características:



Figura 42: Regla creada

## 6.2 RESULTADOS CORTAFUEGOS

Una vez se han configurado y guardado estos parámetros, al momento de ejecutar una conexión vía web se obtendrá un timed out en el explorador web, que nos indica que la regla ha sido ejecutada e impide la conexión:



Figura 43: Respuesta explorador Web

Respuesta explorador Web Ahora, puesto que la regla ha sido creada con el servicio que tiene en cuenta protocolo TCP/UDP bajo puertos 80 y 443, la respuesta de ping no será afectada:

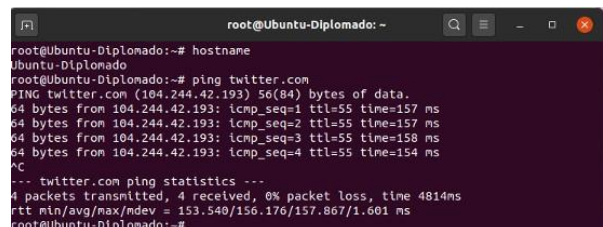


Figura 44: Respuesta ping

## 7. TEMÁTICA 4: FILE SERVER Y PRINT SERVER

Implementación y configuración detallada del acceso de una estación de trabajo GNU/Linux a través del controlador de dominio LDAP a los servicios de carpetas compartidas e impresoras

Se realizará la instalación del rol del servidor como controlador de dominio LDAP a los servicios de carpetas compartidas e impresoras, donde se definen los paquetes que son necesarios para establecer el servidor como controlador de dominio y compartición de ficheros.



Imagen 45. Instalación completa Zentyal

Una vez finalizada la instalación y haber realizado la verificación de que el módulo de controlador de dominio y compartición de ficheros este activo, ya podemos navegar por la sección de usuarios y equipos, allí es donde se puede crear tanto usuarios, grupos y unidades organizativas.

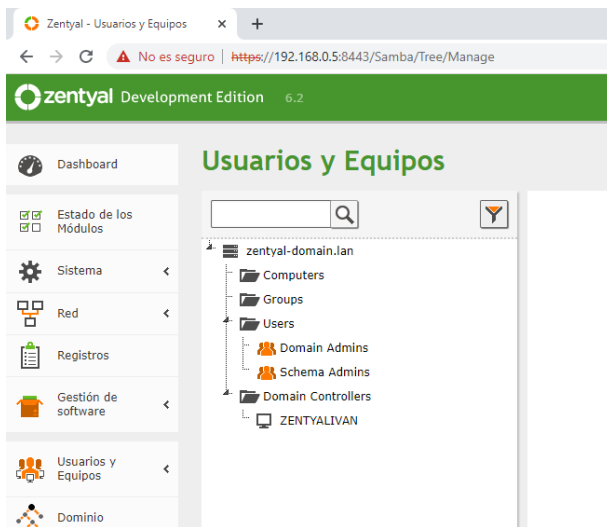


Imagen 46. Sección de Usuarios y Equipos

Antes de compartir cualquier fichero se debe crear un usuario, grupo o lista de usuarios dentro de una unidad organizativa, el cual se encuentra en la sección de Usuarios y Equipos y una vez allí en el árbol de usuario

podemos crearlos según la estructura que la organización requiera.

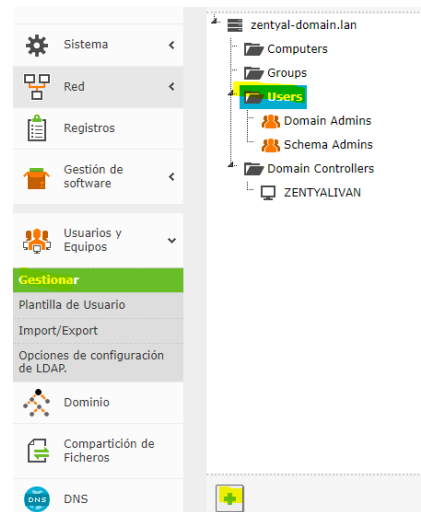


Imagen 47. Árbol de usuarios

Adicionalmente una vez creado el usuario se debe recordar que cada uno de estos se le crea un directorio personal /home/<nombredeusuario> en el servidor, por lo cual el directorio será accesible al usuario (y sólo al usuario) usando SMB/CIFS.

Dentro de la sesión de Compartición de Ficheros, ya podemos proceder con la creación del recurso que se va a compartir, allí se diligencian los datos de la plantilla, donde se indica un nombre al recurso compartido, la ruta bajo que directorio estará gestionado, según el siguiente ejemplo:

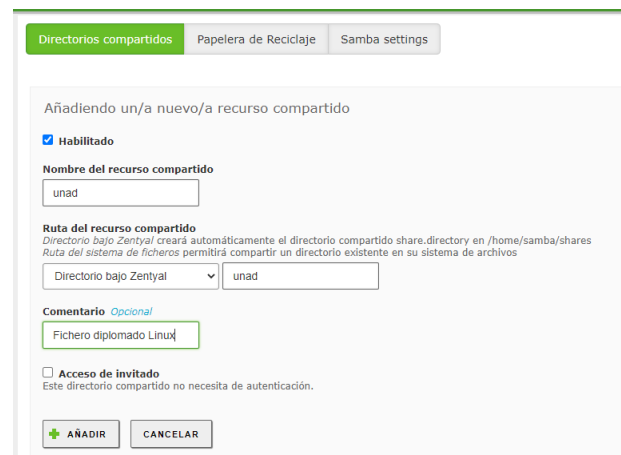


Imagen 48. Directorio compartido

Es de aclarar que se pueden parametrizar como la papelera reciclable de este recurso compartido, configurar los logs de la samba. Los directorios compartidos pueden ser gestionados accediendo a Control de Acceso (ACL), allí se gestionan la asignación de permisos con los diferentes privilegios como lo es, lectura, lectura escritura o administrador a usuarios y grupos.



Imagen 49. Permisos ACL

Una vez creado el recurso compartido, ya se puede ingresar a este desde un equipo cliente, es de aclarar, que los equipos cliente se pueden vincular al controlador de dominio, generando relación de confianza entre los dos, pero también se puede acceder a este sencillamente con las credencial de acceso de un usuario creado en el LDAP, por ejemplo en este caso se utilizara un equipo bajo plataforma Windows, donde se accede al recurso compartido por medio de la dirección IP del servidor y con las credenciales de autenticación de un usuario con permisos.

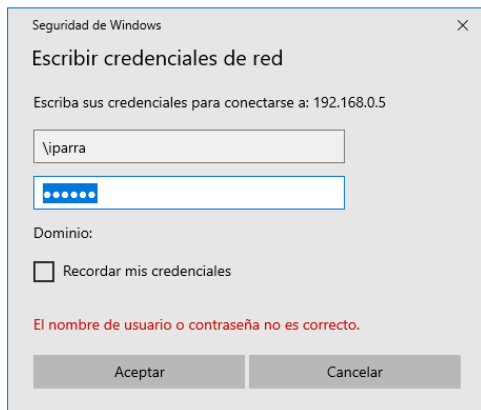


Imagen 50. Acceso a recurso compartido

Ahora ya se puede acceder y ver los recursos compartidos que tiene ese usuario dentro del servidor de Zentyal, adicionalmente se puede ver el directorio personal /home/<nombredeusuario> del usuario, es decir, ya podemos realizar acciones sobre del fichero compartido, teniendo en cuenta los permisos asignados en los ACL.

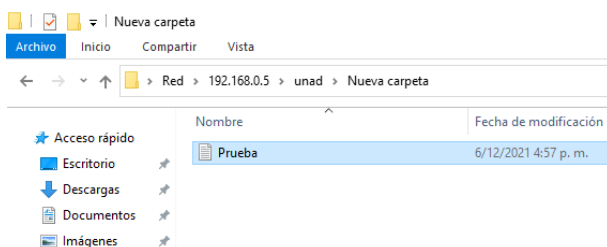


Imagen 51. Prueba de archivos

Es importante entender que esta estructura del Zentyal, la podemos visualizar dentro de un terminal en el

servidor, es decir es totalmente gestionable por medio de comandos, como lo podemos ver en esta imagen.

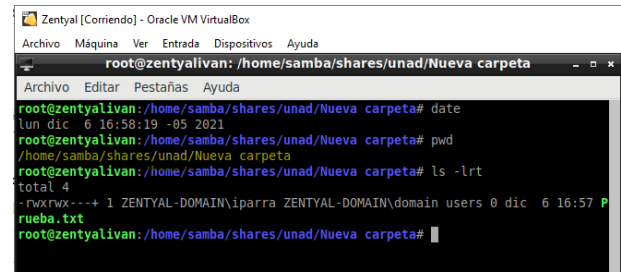


Imagen 52. Zentyal en terminal

## 8. CONCLUSIONES

Al gestionar Zentyal se demuestra el funcionamiento con los servicios de red protegida por el firewall Endian. Los clientes de la red se enlazan al dominio local a través del servidor DNS que resuelve las solicitudes almacenándola en cache por cada petición durante un período de tiempo determinado reduciendo el tiempo de cada la conexión de red y el consumo de tráfico hacia Internet.

El servidor DHCP conectar los dispositivos con una asignación automática de direcciones de red, al solicitar la configuración IP el servidor recurre a una base de datos que contiene los parámetros de red asignables con los rangos de direcciones IP disponibles para ser concedidos en la interfaz de red.

Por medio de la configuración de elementos como Servicios y Objetos, la gestión de las reglas del cortafuegos permite una administración organizada y centralizada, evitando crear reglas repetitivas sobre elementos individuales ya que se pueden agrupar. Por otra parte, se debe tener sumo cuidado con cada uno de los parámetros de las reglas en el cortafuegos, con el fin de evitar el bloqueo a servicios que deben encontrarse abiertos y pueden afectar directamente la operación de la compañía.

Es evidente el avance que presentan las distribuciones Linux, el trabajo de desarrolladores y programadores brindan a los usuarios alternativas de fácil manejo con herramientas muy completas para desarrollar labores de escritorio o de servidor, como en este caso con la distribución Zentyal; la cual cuenta con una amplia documentación que permite fácilmente su configuración.

## 9. REFERENCIAS

- [1] Ruiz, P. (2020, septiembre 14). Establecer una dirección IP estática en Ubuntu Server 20.04. Somebooks.es. <http://somebooks.es/establecer-una-direccion-ip-estatica-en-ubuntu-server-20-04/>
- [2] (S/f). Zentyal.org. Recuperado el 2 de diciembre de 2021, de

<https://doc.zentyal.org/es/installation.html#instalacion-sobre-ubuntu-20-04-lts-server-o-desktop>.

- [3] Experiencia con Zentyal. Diciembre de 2017. Recuperado de <https://blog.desdelinux.net/miexperiencia-con-zentyal/>
- [4] Servicio de Proxy HTTP Documentación de Zentyal 7.0. Recuperado de <https://doc.zentyal.org/es/proxy.html>
- [5] Zentyal 7.0 Documentación Oficial Documentación de Zentyal 7.0. [doc.zentyal.org](https://doc.zentyal.org/es/) recuperado de <https://doc.zentyal.org/es/>
- [6] ZENTYAL. Cortafuegos. [En línea]. Disponible en: <https://doc.zentyal.org/es/firewall.html>