

IMPLEMENTACIÓN DE SERVICIOS PARA LA MIGRACIÓN POR MEDIO DE ZENTYAL SERVER

Leandro Critiano Mendivelso
lcristianom@unadvirtual.edu.co
Fredy Esteban Cely Rojas
fecelyr@unadvirtual.edu.co
Luis Gabriel Español Soracá
espanalg@gmail.com
Harold Jesith Rojas Becerra
hjrojasbe@unadvirtual.edu.co

RESUMEN: *Zentyal es un proyecto open source con el que vamos a realizar diferentes tareas para la migración que se está llevando a cabo a una empresa y contar con un servidor Linux que por medio de la instalación de módulos con los podemos administrar y gestionar los recursos con el fin de brindar una experiencia amigable desde su interfaz de usuario.*

Por medio de este servidor se ha implementado el manejo de servicios que se encuentran en cada temática de la actividad entre las cuales están: puesta en marcha de servicios DHCP Server, DNS Server y controlador de dominio, proxy no transparente, cortafuegos, file server y print server, y la implementación y configuración de una VPN.

PALABRAS CLAVE: Cortafuegos, DHCP server, DNS Server, File, server y Print Server, VPN, Zentyal.

1 INTRODUCCIÓN

En las operaciones para gestionar y adaptar infraestructura tecnológica existen gran variedad de herramientas, nosotros como hemos venido haciendo una migración hacia un sistema GNU/Linux vamos a implementar un servidor Zentyal con el que podemos administrar de forma eficiente los servicios que necesitan nuestra empresa y poder brindar un soporte a cada una de sus demandas anteriormente planteadas y estudiadas.

2 INSTALACION DE ZENTYAL SERVER

El proceso de instalación se realiza sobre una máquina virtual, los requisitos mínimos varían según el tipo de

servicios que se despliegan, a continuación se describe el proceso de instalación:

el software que vamos a instalar lo descargamos desde su web oficial que podemos acceder por medio del siguiente link:

Link: <https://zentyal.com/es/comunidad/>

Creamos la máquina virtual

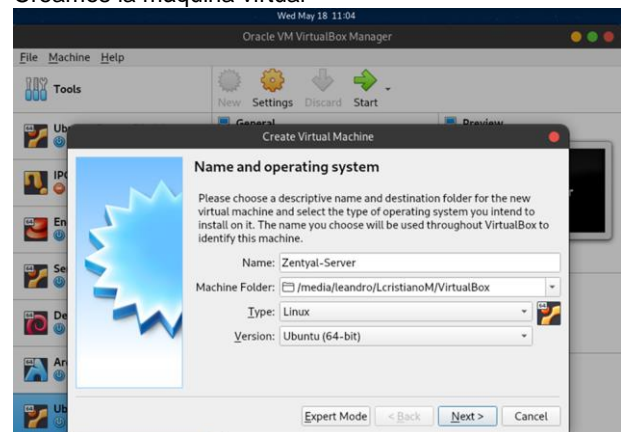


Figura 1 - creamos la máquina virtual para Zentyal - autoría propia

Asignamos la memoria RAM para la máquina

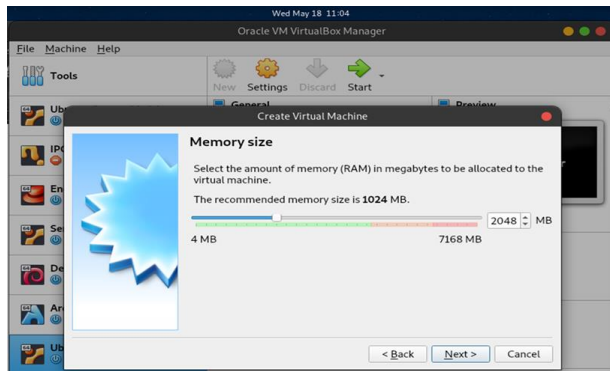


Figura 2 - asignamos el espacio para la RAM - autoría propia

Asignamos el espacio en disco que vamos a darle a la máquina



Figura 3 - asignamos espacio de disco - autoría propia

Iniciamos nuestra máquina configurada

Elegimos el idioma que vamos a usar para nuestro servidor

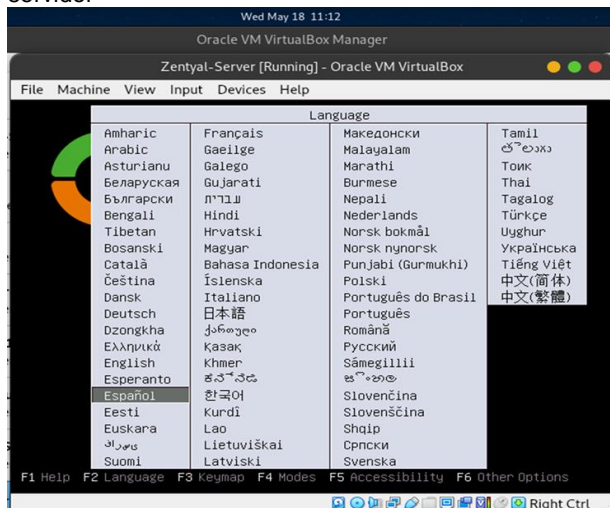


Figura 4 - elegimos idioma para la instalación - autoría propia

Seleccionamos la opción de instalación de la versión de Zentyal



Figura 5 - opción a instalar - autoría propia

Seleccionamos español para el idioma de teclado

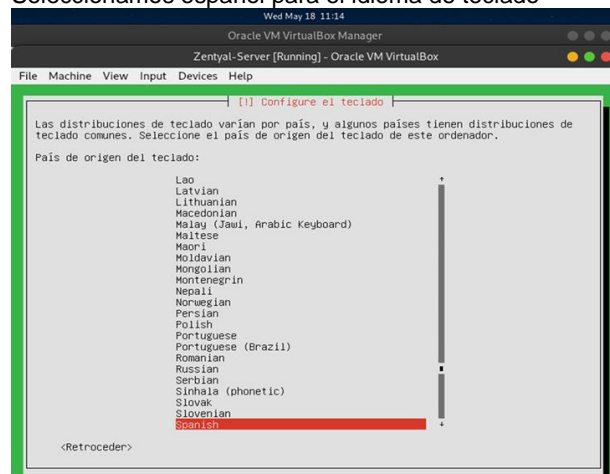


Figura 6 - distribución de teclado - autoría propia

Asignamos nombre a la máquina para identificarla en la red.

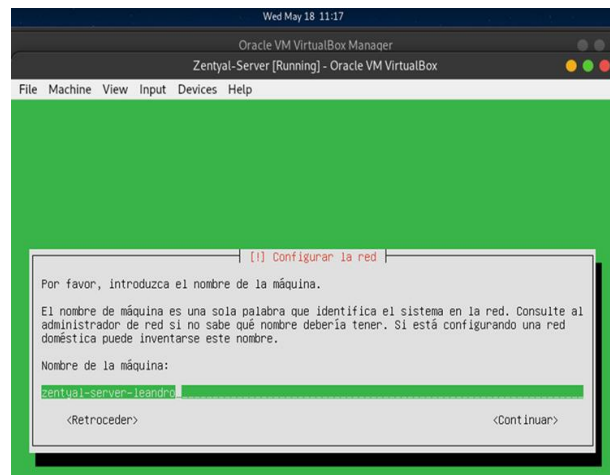


Figura 7 - nombre de la máquina - autoría propia

Nombre de usuario para la cuenta

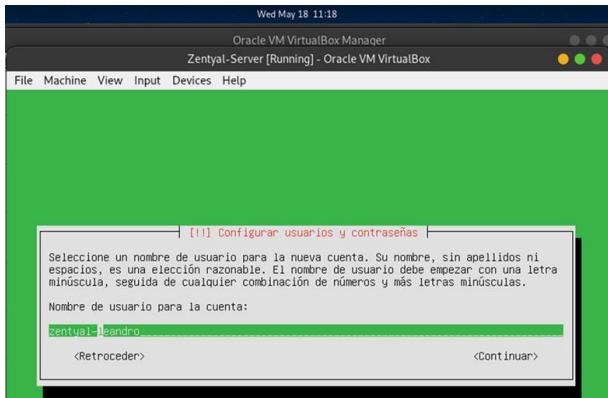


Figura 8 - nombre de la cuenta - autoría propia

Configuramos contraseña para la cuenta.

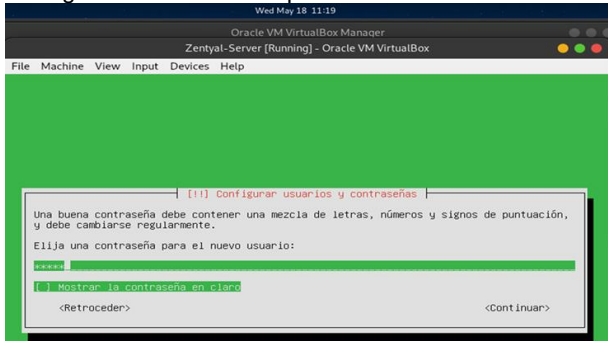


Figura 9 - contraseña de la cuenta - autoría propia

Inicia proceso de instalación

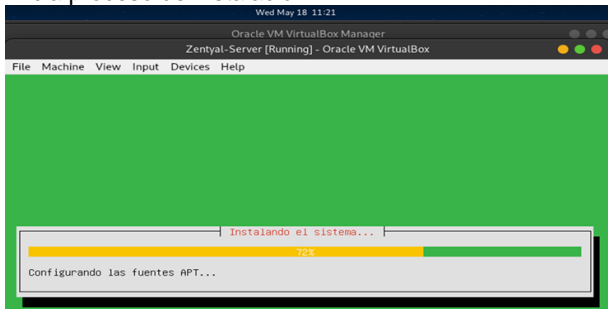


Figura 10 - inicio de la instalación - autoría propia

Se descarga el cargador de arranque grub.

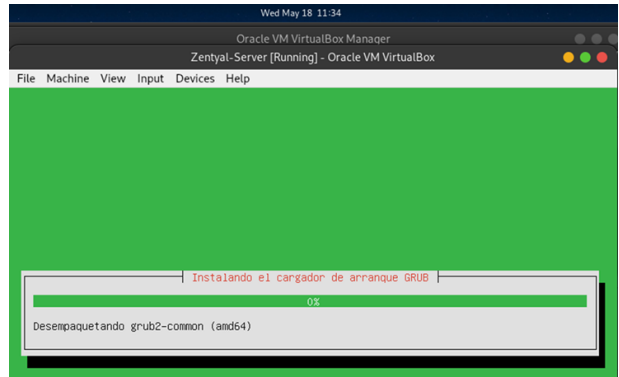


Figura 11 - instalación de GRUB - autoría propia

Inicia nuestra máquina.



Figura 12 - inicio de la máquina - autoría propia

Ingresamos a la página de Zentyal.

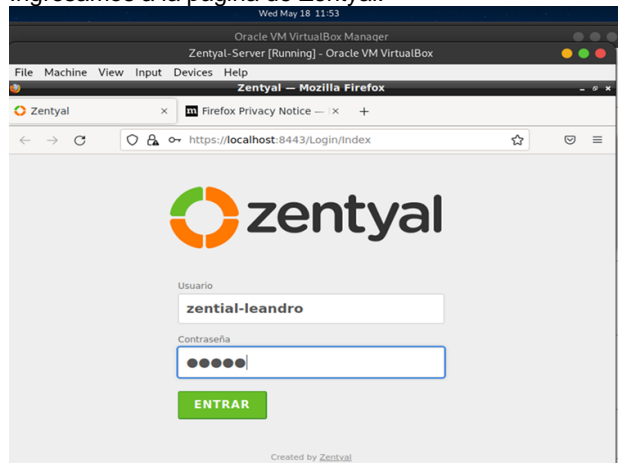


Figura 13 - página inicial Zentyal - autoría propia

Instalación de servicios

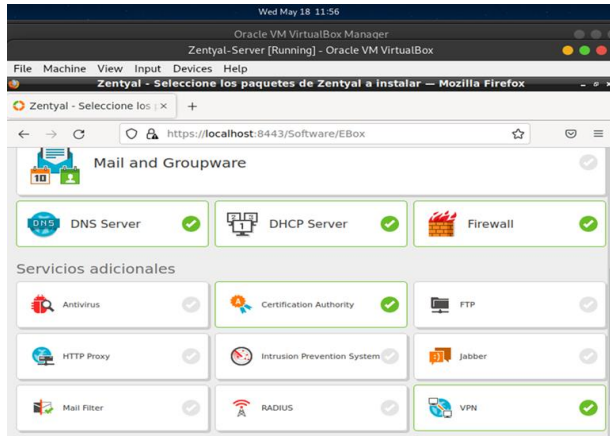


Figura 14 - módulos a instalar - autoría propia



Figura 16- Instalación de paquetes

TEMÁTICA 2: PROXY NO TRANSPARENTE

Producto esperado: Implementación y configuración detallada del control del acceso de una estación GNU/Linux a los servicios de conectividad a Internet desde Zentyal a través de un proxy que filtra la salida por medio del puerto 1320

Seleccionamos instalar los paquetes que necesitamos para el desarrollo de nuestra temática.

Seleccionamos el tipo de servidor y nombre del dominio



Figura 17- Selección de servidor

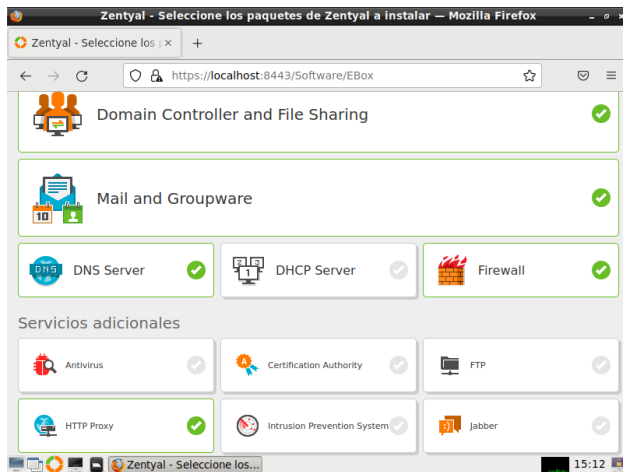


Figura 15-Paquetes a instalar

Proceso de instalación de los paquetes seleccionados

Vemos nuestro dashboard como página principal de zentyal

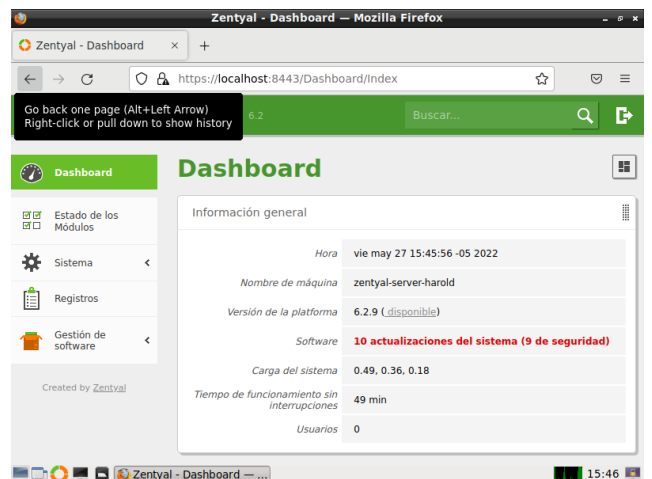


Figura18 – Dashboard Zentyal

Verificamos que todos los paquetes si se hallan instalado en zentyal

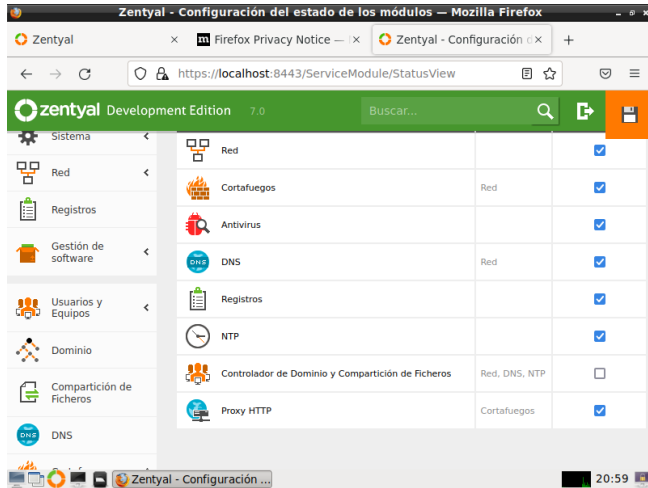


Figura 19 – paquetes instalados

Configuramos nuestro servidor proxy no transparente con puerto 1320 como lo requiere la guía.

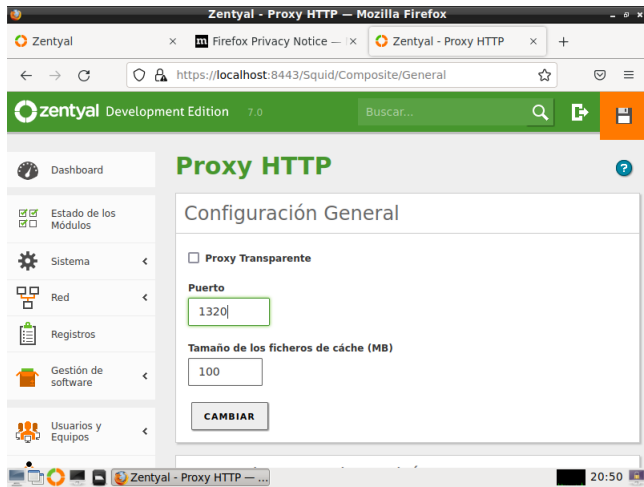


Figura 20 – Configuración Proxy

Verificamos la dirección Ip asignada a nuestro servidor zentyal

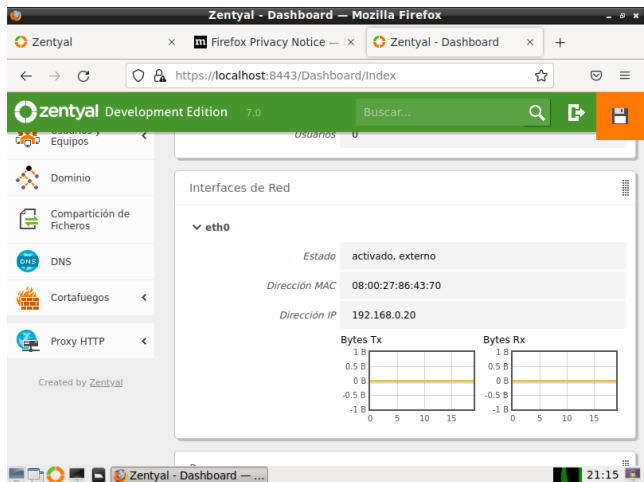


Figura 21 – Direccionamiento Servidor

Añadimos un nuevo perfil de filtrado

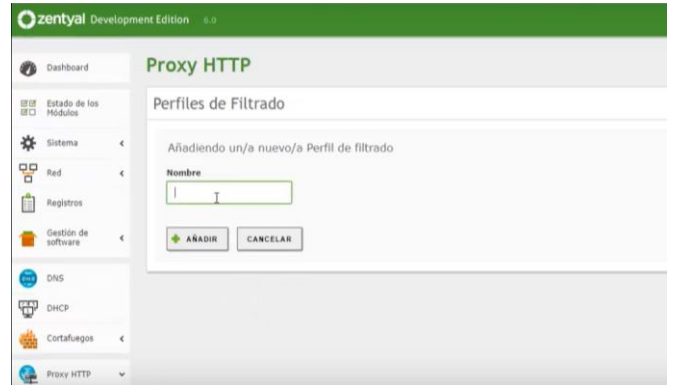


Figura 22 – Pefiles de filtrado

En reglas de dominios y Urls denegamos el acceso a la página de Facebook a través del servidor proxy

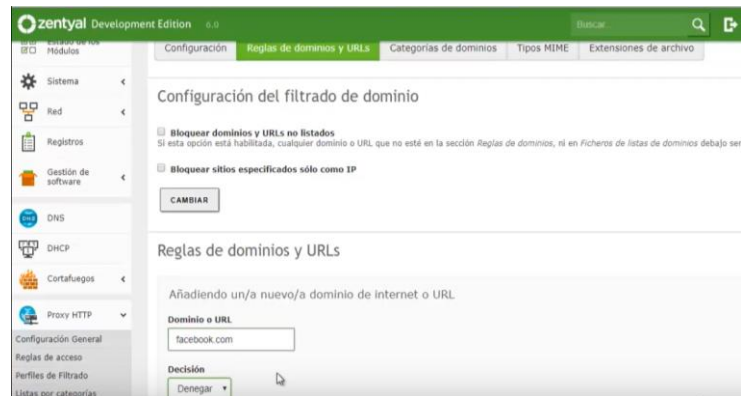


Figura 23 – Reglas de dominio

En nuestra máquina de cliente en la configuración de Firefox, activamos nuestro proxy de red con la dirección Ip de nuestro servidor y el puerto correspondiente.

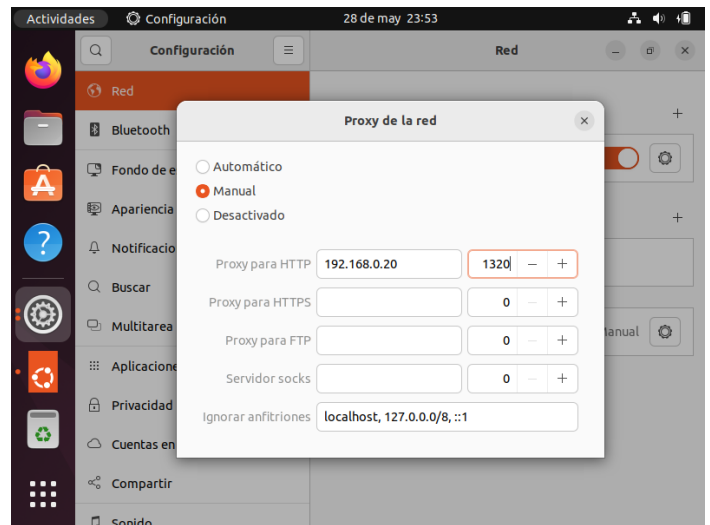


Figura 24 – Configuración proxy en navegador

Ingresamos a la página de Facebook desde el navegador de nuestro cliente, donde se puede ver que se niega el acceso demostrando el funcionamiento del proxy no transparente.

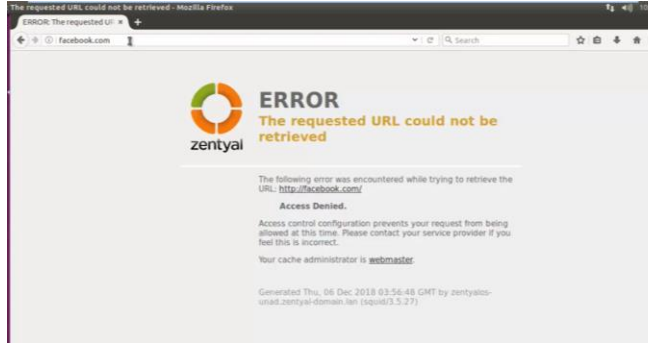


Figura 25 – Acceso denegado Facebook

TEMÁTICA 3: CORTAFUEGOS

Producto esperado: 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

Configuro eth0 como Externa



Figura 26 Puerto de red 1

Tipo de red DHCP



Figura 27 Puerto de red 2

Y eth1 como interna (LAN) con IP estática 192.168.1.254



Figura 28 Puerto de red 1 se asigna IP

Configuro en nuestro cliente Ubuntu la puerta de enlace y servidor DNS para que se conecte a Internet a través de Zentyal.

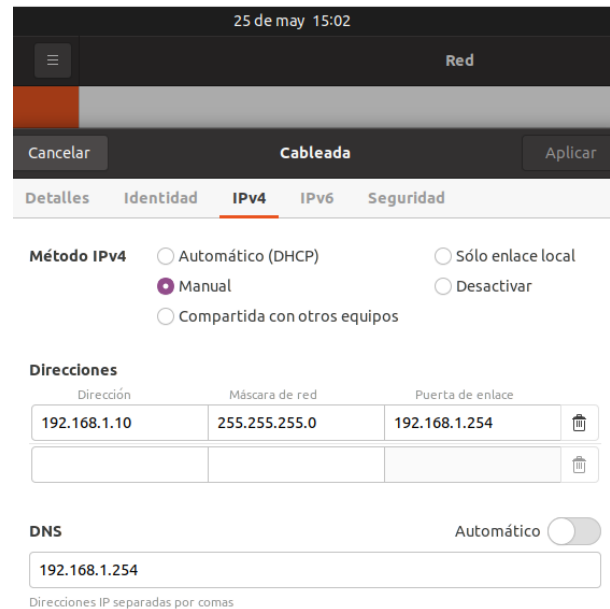
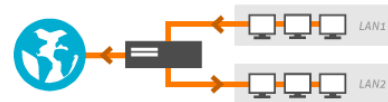


Figura 29 configuración de la red en el cliente

En Zentyal se configura el filtro de paquetes en el cortafuegos para las redes internas



Reglas de filtrado para las redes internas

Estas reglas le permiten controlar el acceso desde sus redes internas a Internet, y el tráfico entre sus redes internas. Si desea dar acceso a los servicios de Zentyal, debe usar la sección superior.



Figura 30 Seleccionar reglas de filtrado para redes

Creamos las reglas que restringen el acceso a las diferentes redes o páginas de entretenimiento



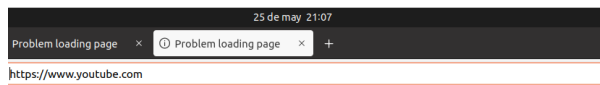
Figura 31 las reglas creadas

Detalle la creación de la regla



Figura 32 Detalle de cada regla

Probando las reglas en el equipo cliente

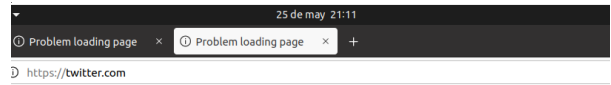


The connection has timed out

The server at www.youtube.com is taking too long to respond.

- The site could be temporarily unavailable or too busy. Try again in a few moments.
- If you are unable to load any pages, check your computer's network connection.
- If your computer or network is protected by a firewall or proxy, make sure that Firefox is permitted to access the Web.

Figura 33 Prueba de la página de YouTube

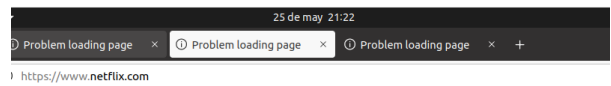


The connection has timed out

The server at twitter.com is taking too long to respond.

- The site could be temporarily unavailable or too busy. Try again in a few moments.
- If you are unable to load any pages, check your computer's network connection.
- If your computer or network is protected by a firewall or proxy, make sure that Firefox is permitted to access the Web.

Figura 34 Prueba de la página de Twitter

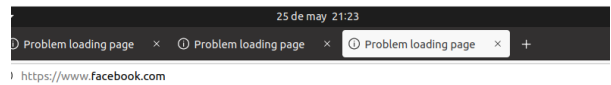


The connection has timed out

The server at www.netflix.com is taking too long to respond.

- The site could be temporarily unavailable or too busy. Try again in a few moments.
- If you are unable to load any pages, check your computer's network connection.
- If your computer or network is protected by a firewall or proxy, make sure that Firefox is permitted to access the Web.

Figura 35 Prueba de la página Netflix



The connection has timed out

The server at www.facebook.com is taking too long to respond.

- The site could be temporarily unavailable or too busy. Try again in a few moments.
- If you are unable to load any pages, check your computer's network connection.
- If your computer or network is protected by a firewall or proxy, make sure that Firefox is permitted to access the Web.

Figura 36 Prueba de la página de Facebook

Detengo las reglas para probar que las páginas funcionan



Figura 37 Permito el acceso

Probando que las páginas funcionan correctamente

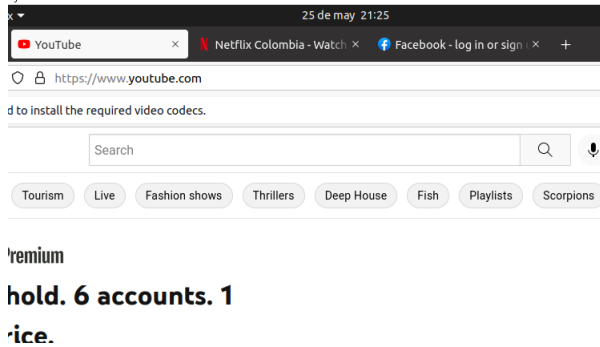


Figura 38 probando la página de YouTube

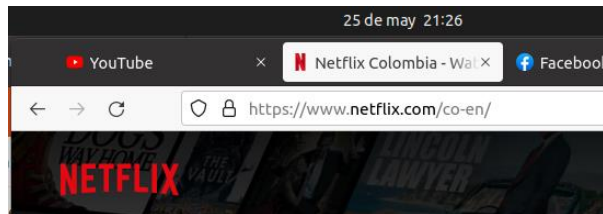


Imagen Probando la página de Netflix

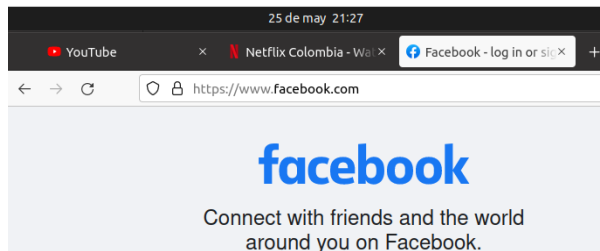


Figura 39 probando la página de Facebook

TEMÁTICA 4: FILE SERVER Y PRINT SERVER

Producto esperado: 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, iniciamos configurando las interfaces de red una por dhcp y otra estatica en la maquina virtual



Figura 40 configuración tarjetas de red

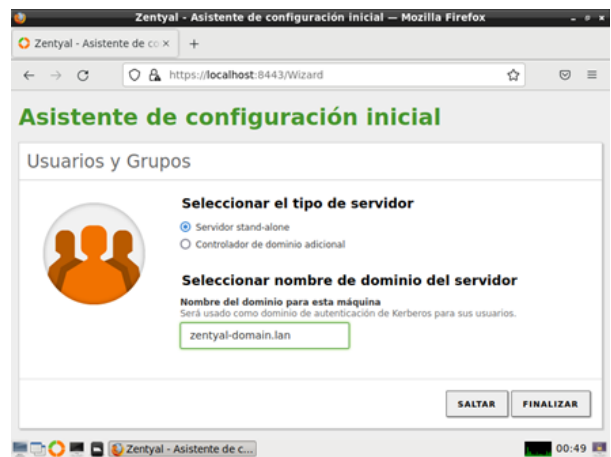


Figura 41 seleccionando el tipo de servidor

TEMÁTICA 5: IMPLEMENTACIÓN DE UNA VPN

Se presentan los resultados obtenidos al realizar la implementación de la vpn.

2.5.1 empezamos con la creación de los certificados necesario con los que podemos realizar las conexiones de manera exitosa

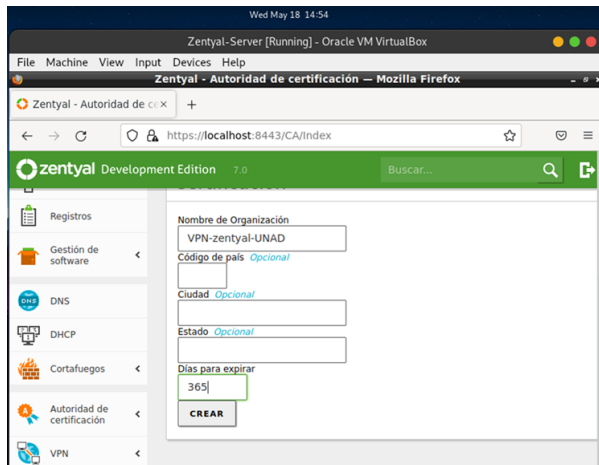


Figura 42- nuevo certificado - autoría propia

2.5.2 Creamos un servidor VPN nuevo con el cual podemos acceder desde nuestro cliente.

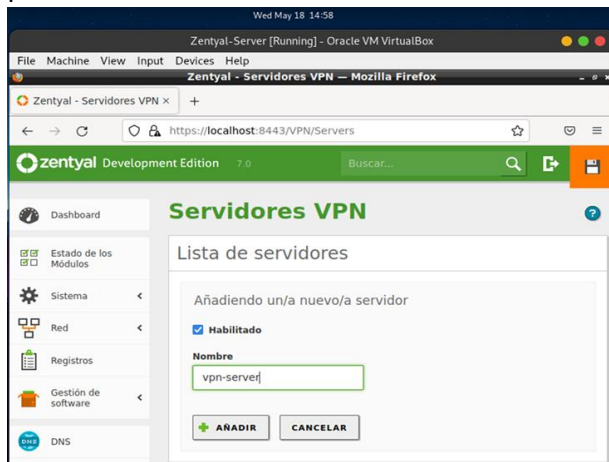


Figura 43- nuevo servidor - autoría propia

2.5.3 Configuramos el servidor.

desde aqui vamos a nombrar el puerto que se va a usar, ademas de la direccion ip que va a contar e ingresamos el certificado que se ha expedido antes, esto nos sirve para que la conexión se realice sin problemas de autenticación.

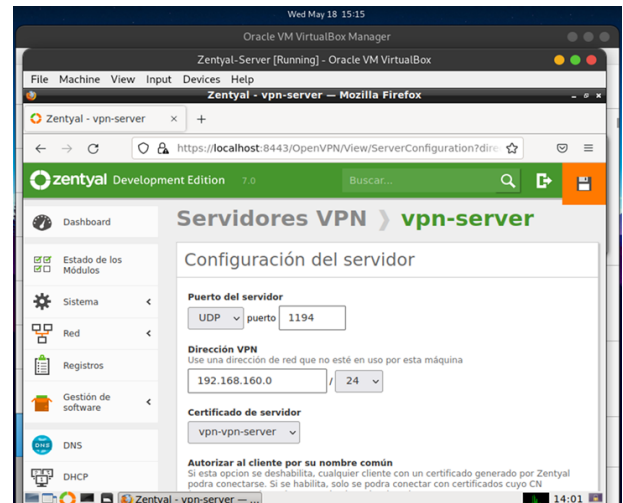


Figura 44- configuración del servidor - autoría propia

2.5.4 Después de guardar las configuraciones vemos que el demonio OpenVPN está funcionando.

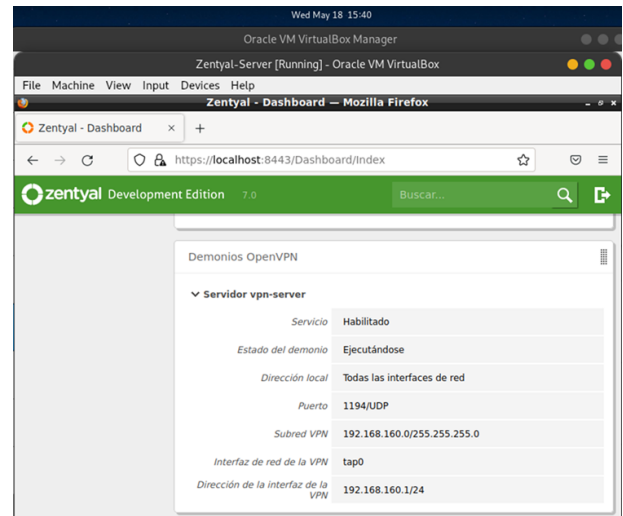


Figura 45- VPN habilitada - autoría propia

2.5.5 En nuestro sistema operativo del cliente vamos a realizar las configuraciones para poder usar la VPN, para ello se instala el módulo de openvpn con el comando sudo apt install openvpn, ubicamos la carpeta que se ha descargado desde zentyal con la que ya tenemos todas las configuraciones realizadas, posteriormente descomprimos el archivo que creamos en Zentyal, a continuación, movemos los fichero a la ruta /etc/openvpn/.

```

debian11 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Aplicaciones Lugares Sistema
leandro@leandrocris: /etc/default
Archivo Editar Ver Buscar Terminal Ayuda
bluetooth dbus hwdm networking saned
root@leandrocris: /etc/default# chmod +w openvpn
root@leandrocris: /etc/default# nano openvpn
root@leandrocris: /etc/default# cd ..
root@leandrocris: /etc# cd ..
root@leandrocris: /# ls
bin home lib32 media root sys vmlinuz
boot initrd.img lib64 mnt run tmp vmlinuz.old
dev initrd.img.old lib32 opt sbin usr
etc lib lost+found proc srv var
root@leandrocris: /# cd home/
root@leandrocris: /home# ls
leandro
root@leandrocris: /home# cd leandro/Descargas/
root@leandrocris: /home/leandro/Descargas# ls
7E03915B807C6001.pem vpn-server-client-VPN-zentia-2.tar.gz
cacert.pem VPN-zentia-2.pem
vpn-server-client.conf
root@leandrocris: /home/leandro/Descargas# mv *.pem /etc/o
openal/ openn12/ opensc/ openvpn/ opt/ os-release
root@leandrocris: /home/leandro/Descargas# mv *.pem /etc/openvpn/
root@leandrocris: /home/leandro/Descargas#

```

Figura 46– configuración de VPN desde desktop - autoría propia

2.5.6 Ejecutamos el comando `sudo openvpn client.conf` para ejecutar la vpn y observamos el resultado de la conexión.

```

debian11 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Aplicaciones Lugares Sistema
leandro@leandrocris: /etc/default
Archivo Editar Ver Buscar Terminal Ayuda
root@leandrocris: /etc/openvpn# sudo openvpn client.conf
2022-05-18 19:17:32 WARNING: Compression for receiving enabled. Compression
s been used in the past to break encryption. Sent packets are not comp
nless "allow-compression yes" is also set.
2022-05-18 19:17:32 DEPRECATED OPTION: --cipher set to 'AES-256-CBC' bu
ng in --data-ciphers (AES-256-GCM:AES-128-GCM). Future OpenVPN version
more --cipher for cipher negotiations. Add 'AES-256-CBC' to --data-cipl
change --cipher 'AES-256-CBC' to --data-ciphers-fallback 'AES-256-CBC'
nce this warning.
2022-05-18 19:17:32 OpenVPN 2.5.1 x86_64-pc-linux-gnu [SSL (OpenSSL)]
[24] [EPOLL] [PKCS11] [MH/PKTINFO] [AEAD] built on May 14 2021
2022-05-18 19:17:32 library versions: OpenSSL 1.1.1n 15 Mar 2022, LZO
2022-05-18 19:17:32 TCP/UDP: Preserving recently used remote address:
]192.168.0.37:1194
2022-05-18 19:17:32 Socket Buffers: R=[212992->212992] S=[212992->2129
2022-05-18 19:17:32 UDP link local: (not bound)
2022-05-18 19:17:32 UDP link remote: [AF_INET]192.168.0.37:1194
2022-05-18 19:17:32 TLS: Initial packet from [AF_INET]192.168.0.37:119
3f702b4 45beaeca
2022-05-18 19:17:32 VERIFY OK: depth=1, O=VPN-zentia-UNAD, CN=VPN-zen
D Authority Certificate
2022-05-18 19:17:32 VERIFY X509NAME OK: O=VPN-zentia-UNAD, CN=VPN-zen
2022-05-18 19:17:33 OPTIONS IMPORT: adjusting link_mtu to 1625
2022-05-18 19:17:33 OPTIONS IMPORT: data channel crypto options modifi
2022-05-18 19:17:33 Data Channel: using negotiated cipher 'AES-256-GCM'
2022-05-18 19:17:33 Outgoing Data Channel: Cipher 'AES-256-GCM' initia
th 256 bit key
2022-05-18 19:17:33 Incoming Data Channel: Cipher 'AES-256-GCM' initia
th 256 bit key
2022-05-18 19:17:33 net_route v4_best_gw query: dst 0.0.0.0
2022-05-18 19:17:33 net_route v4_best_gw result: via 192.168.0.1 dev e
2022-05-18 19:17:33 ROUTE_GATEWAY 192.168.0.1/255.255.255.0 IFACE=enp0
R=08:00:27:70:0b:dd
2022-05-18 19:17:33 TUN/TAP device tun0 opened
2022-05-18 19:17:33 net_iface_mtu_set: mtu 1500 for tun0
2022-05-18 19:17:33 net_iface_up: set tun0 up
2022-05-18 19:17:33 net_addr_ptp_v4_add: 192.168.160.6 peer 192.168.16
tun0
2022-05-18 19:17:33 net_route v4_add: 192.168.160.1/32 via 192.168.160
NULL] table 0 metric -1
2022-05-18 19:17:33 WARNING: this configuration may cache passwords in
-- use the auth-nocache option to prevent this
2022-05-18 19:17:33 Initialization Sequence Completed

```

Figura 47- conexión exitosa - autoría propia

3 Conclusiones.

Las conexiones a través de las VPN son altamente demandadas ya que les da un tratamiento diferente a las credenciales de los clientes, todo esto gestionado en este caso por el servidor Zentyal y con el que podemos asignar una dirección ip a un cliente que esté en cualquier parte, solo conectando a servidores se puede hacer este tipo de operaciones.

Los cortafuegos en servidor Zentyal son muy útiles ya que restringen el acceso a las páginas que uno desee como también a qué equipo se le establecen estas reglas Y con ello mejoramos nuestro ancho de banda y garantizamos el no uso desiertas paginas

Un servidor Proxy no transparente nos garantiza mucha más seguridad en la navegación web de nuestros usuarios cliente que tenemos bajo nuestro dominio que un servidor proxy transparente.

4 REFERENCIAS

- [1] Servicio de redes privadas virtuales (VPN) con OpenVPN — Documentación de Zentyal 6.2. (s. f.). Recuperado 21 de mayo de 2022, de <https://doc.zentyal.org/6.2/es/vpn.html>
- [2] Pronger TV. (2019, diciembre 13). Cómo instalar y configurar un servidor VPN en Zentyal—Tutorial 2020. <https://www.youtube.com/watch?v=8zaxU1C7qBc>.
- [3] Cortafuegos — Documentación de Zentyal 7.0. (2021). Zentyal. <https://doc.zentyal.org/es/firewall.html#configuracion-de-un-cortafuegos-con-zentyal>
- [4] Gomez, R. (2013). *Estado del arte de los gestores de ventanas en GNU/Linux, TFC – GNU/Linux*. Paginas (12-19). OpenAccess. <http://openaccess.uoc.edu/webapps/o2/bitstream/10609/19172/7/raulgomezTFC0113memoria.pdf>