SOLUCIONANDO NECESIDADES ESPECÍFICAS CON GNU LINUX/ZENTYAL.

David Guillermo Pérez Amaya
e-mail: dperezam@unadvirtual.edu.co
William Gerardo González Vivas
e-mail: wggonzalezv@unadvirtual.edu.co
Miguel Ángel Barahona Ordoñez
e-mail: mabarahonao@unadvirtual.edu.co
Omar Edilson Infante Peña
e-mail: oeinfantep@unadvirtual.edu.co
Victor Andres Sanchez Veloza
e-mail: vasanchezv@unadvirtual.edu.co

RESUMEN: *En la actualidad el mundo se ha vuelto completamente cambiante, principalmente en temas de tecnologías de información, incluyendo temas relacionados con networking y la seguridad de la información compartida en las redes empresariales.*

En este artículo se aborda la implementación de diferentes servicios bajo Zentyal Server como plataforma de administración de la infraestructura en una organización, se explicará la importancia de esta herramienta instalando y validando el funcionamiento de servicios DHCP, DNS, Controlador de dominio, Proxy, Cortafuegos, PrintServer y VPN.

PALABRAS CLAVE: Conexión, Máquina, Paquetes, Servidor Zentyal.

1 INTRODUCCIÓN

Este artículo se encamina en cómo instalar y configurar un servidor Linux bajo Zentyal que permita brindar un adecuado soporte tecnológico en una empresa que requiera de estas configuraciones. Se evidenciará el manejo del servidor y su alistamiento para aplicar lo aprendido para la implementación de servicios de IT de mayor nivel para intranet y extranet en instituciones complejas.

2 GNU/LINUX ZENTYAL 6.2 SERVER

2.1 INSTALACION ZENTYAL

Una vez descargada la versión 6.2 de Zentyal y con el ISO ejecutándose en la máquina, se botea por la misma.

A continuación, se selecciona el idioma

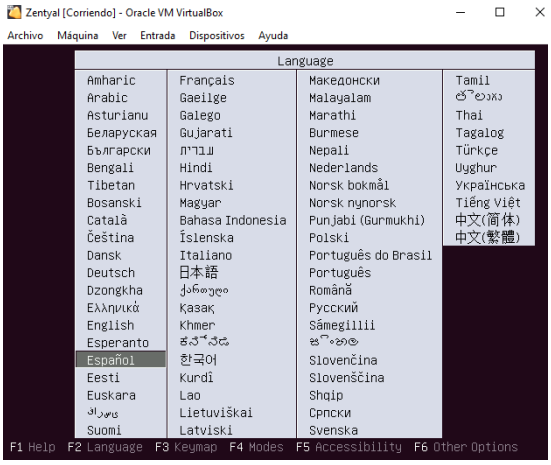

Imagen 1. Selección de idioma

Se elige la opción de instalación que mejor se adapte al servidor. En este caso se usará todo el disco duro.

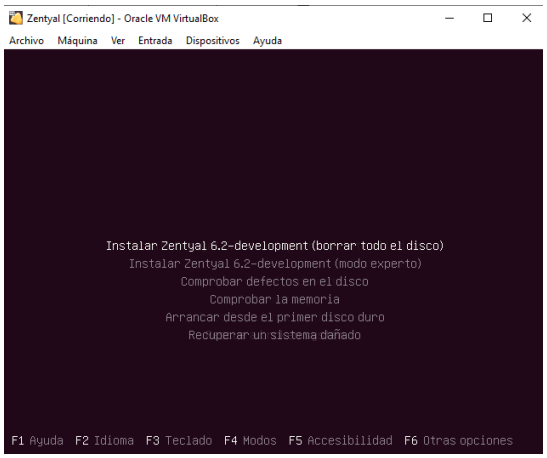

Imagen 2. Modo de instalación

Se selecciona la ubicación y distribución de teclado.

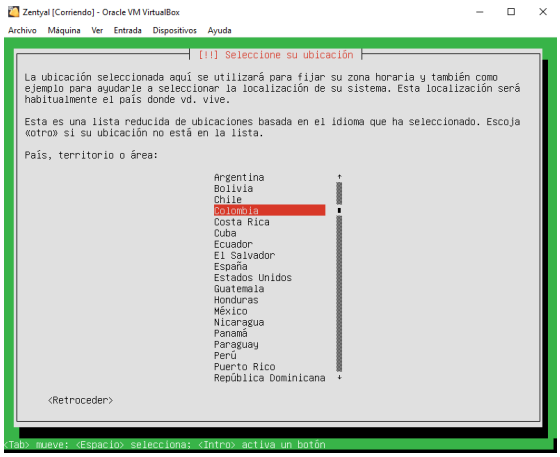

Imagen 3. Ubicación

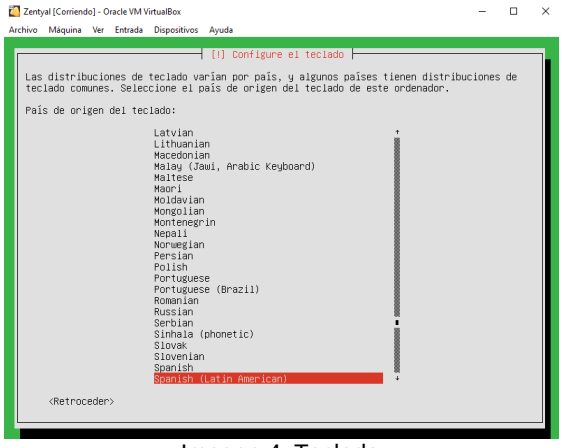

Imagen 4. Teclado

Se configura el usuario administrador y su contraseña.

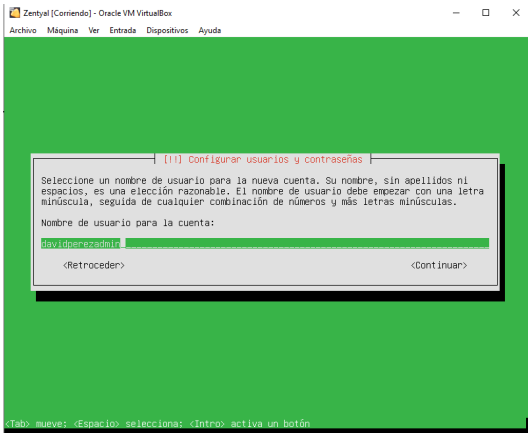

Imagen 5. Usuario administrador

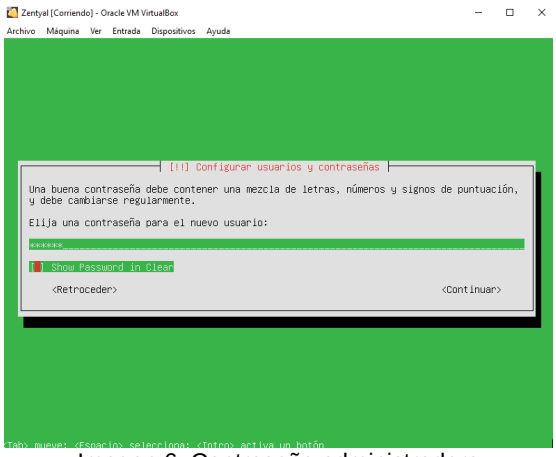

Imagen 6. Contraseña administradora

Una vez se finalice la instalación del servidor Zentyal, se retira el disco y se espera que bootee normalmente el equipo. Al terminar de instalar paquetes opcionales, se podrá ingresar con el usuario y contraseña previamente configurados

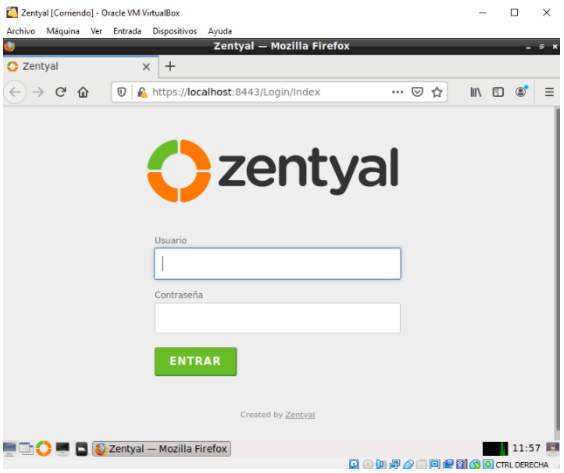

Imagen 7. Ingreso servidor

Imagen 8. Pantalla de bienvenida

2.2 TEMÁTICA 1: DHCP SERVER, DNS SERVER Y CONTROLADOR DE DOMINIO

Temática desarrollada por el estudiante David Guillermo Perez Amaya.

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

Se debe activar los módulos DHCP, DNS, Red y controlador de Dominio.

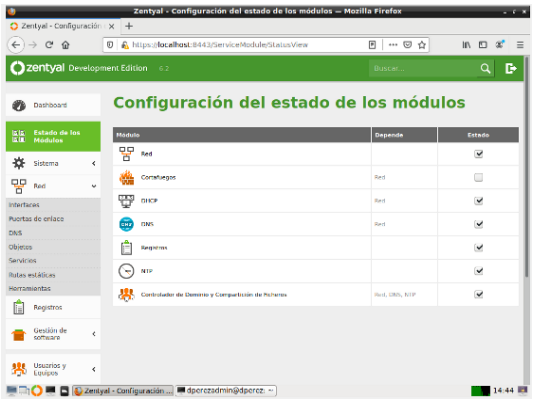

Imagen 9. Activación módulos

Una vez termina la activación de módulos, se configura el adaptador eth0 con DHCP y se habilita la conexión externa WAN.

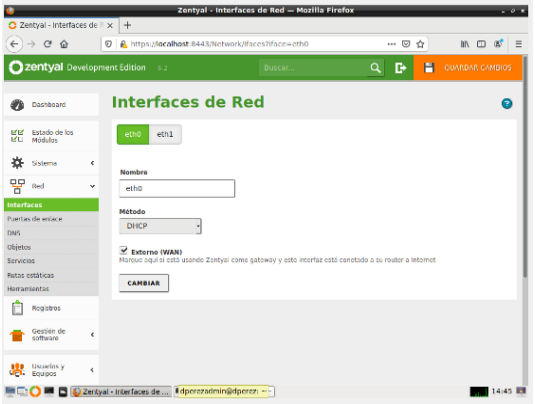

Imagen 10. Configuración DHCP

Luego se configura la Ip estática para el adaptador eth1 según la segmentación de red dada por el administrador.

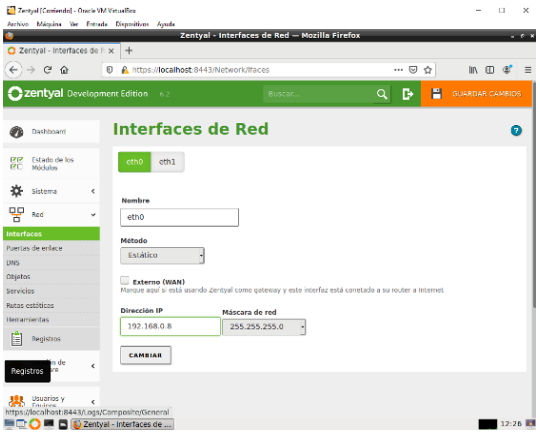

Imagen 11. Configuración Ip estática

En la configuración de red, es necesario definir el objeto con el que posteriormente se va a buscar el servidor.

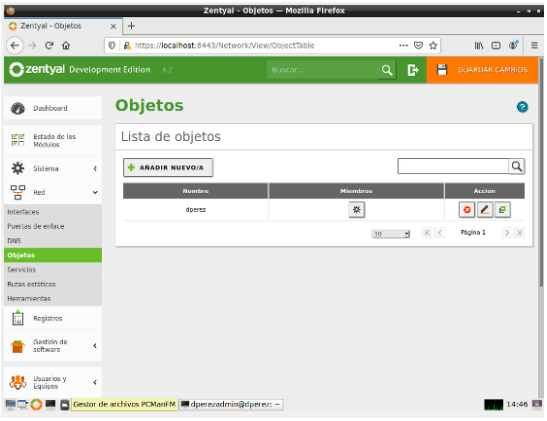

Imagen 12. Definición de objeto

Dentro de la configuración de DHCP, se deben definir los rangos de ip que van a ser asignadas con los equipos que se conectarán a través del Zentyal.

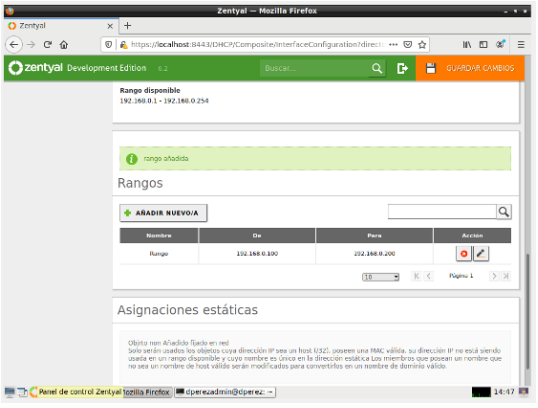

Imagen 13. Rango de Ip a asignar

Asignar el objeto estático con el cual se va a buscar posteriormente el servidor.

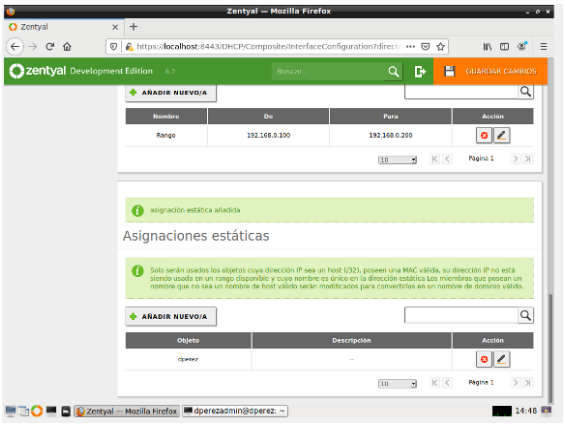

Imagen 14. Objeto estático

En la configuración de red, se configura el dominio de búsqueda del servidor Zentyal.

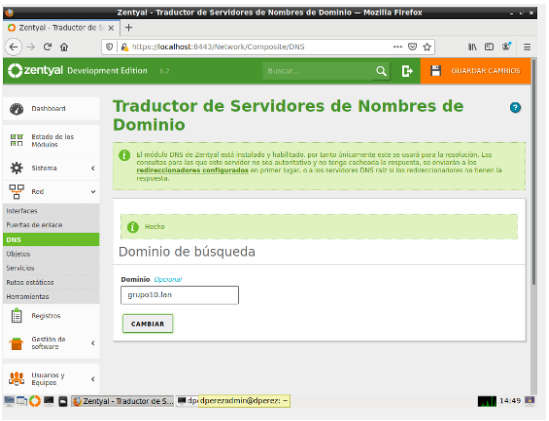

Imagen 15. Dominio de búsqueda

Se configura el redireccionado, en este caso se usarán los dns de google 8.8.8.8.

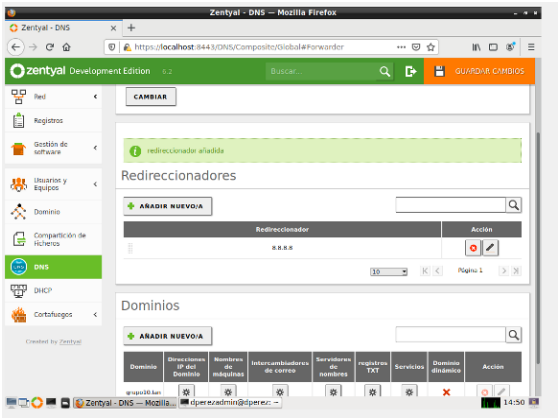

Imagen 16. Redireccionador

En la configuración de DNS, se añade el dominio del servidor. En este ejemplo es dperez.dns.

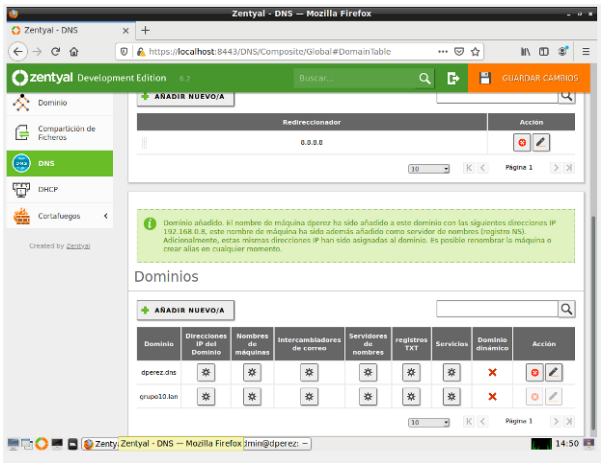

Imagen 17. Dominios configurados

Se guardan todos los cambios para que sean aplicados en el servidor Zentyal.

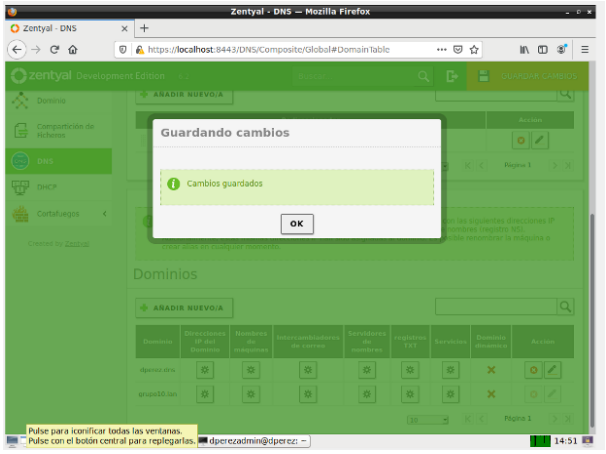

Imagen 18. Guardado de cambios

En una máquina virtual o equipo host que se encuentre en la misma red interna del servidor Zentyal, se crea un nuevo perfil cuya ip debe ser asignada dinámicamente por DHCP.

Imagen 19. Perfil DHCP nuevo

Se debe asegurar que la ip asignada al nuevo equipo se encuentre dentro del rango de ips previamente configurada en el apartado de DHCP.

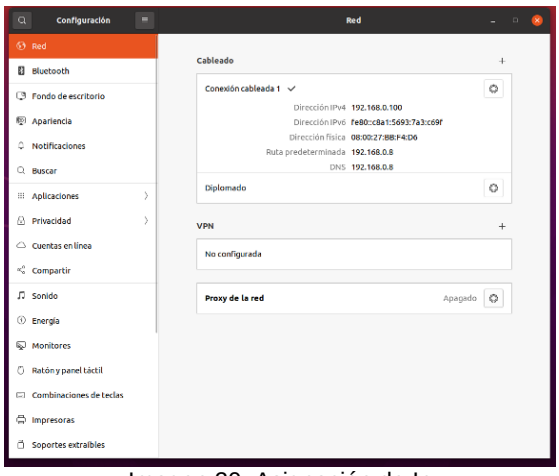

Imagen 20. Asignación de Ip

A continuación, se realiza prueba de ping al servidor Zentyal tanto con la ip como con el dominio.

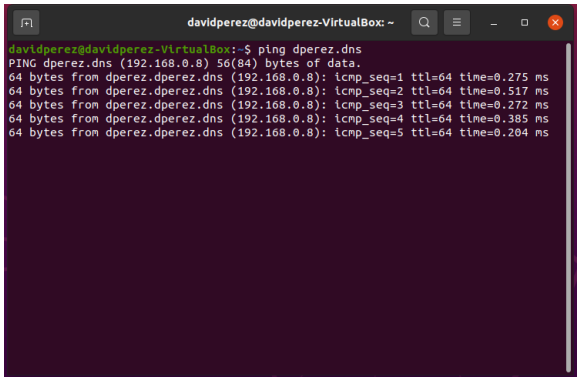

Imagen 21. Prueba desde equipo desktop

Dentro de la configuración de usuarios y equipos, se configura un nuevo grupo de distribución llamado diplomado.

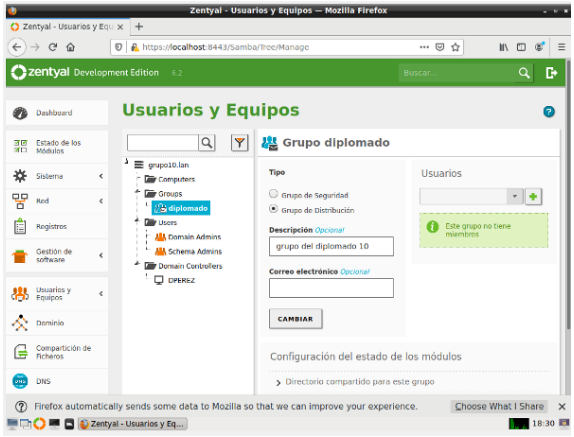

Imagen 22. Creación de grupo

Dentro del mismo menú, se crea el usuario de prueba y se asigna al grupo de diplomado.

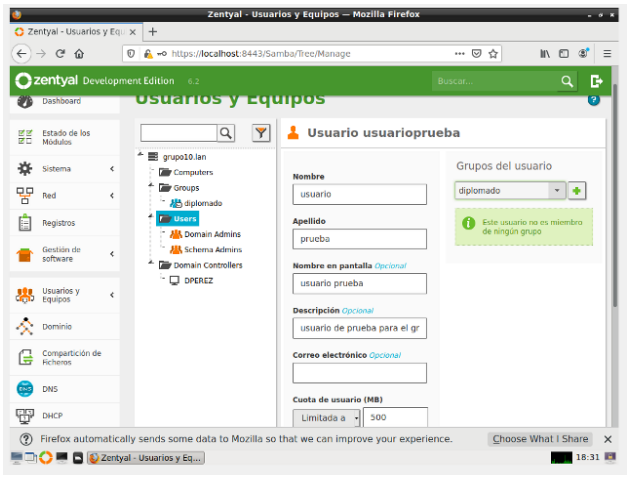

Imagen 23. Creación de usuario

Por último, se realiza la prueba de ingreso desde el equipo desktop en el navegador con el dominio creado para tal fin.

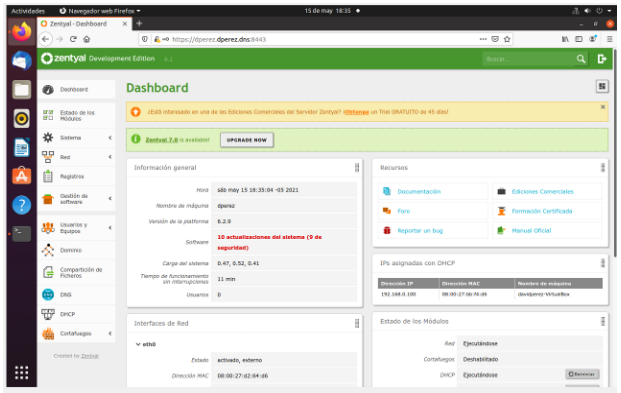

Imagen 24. Prueba en equipo desktop

2.3 TEMÁTICA 2: PROXY NO TRANSPARENTE

Temática desarrollada por el estudiante William Gerardo González Vivas

La optimización de recursos, mantener el performance y la seguridad en las redes de cómputo de las empresas son tareas fundamentales en la administración de un sistema. Aspectos clave como la reducción del uso del ancho de banda, mejora los tiempos de respuesta en las consultas a sitios web, filtración de contenido, control el acceso a sitios web y fortalecimiento de la seguridad de la red normalmente son manejados mediante herramientas software y Hardware como Firewalls, UTM (Unified Thread Management o Gestión Unificada de Amenazas), soluciones eficientes, pero son costosas y complejas de manejar. Afortunadamente, soluciones de código abierto como Zentyal es posible cubrir estos aspectos de forma sencilla y a través de una

única plataforma y sobre una interfaz visual, mediante los módulos Firewall y Proxy HTTP. En este artículo, tratará de mostrar la configuración e implementación de un Proxy HTTP en un servidor Zentyal 6.2., tomando como base el siguiente diagrama de red de máquinas virtuales creadas con VirtualBox:

Diagrama de red – Servicio Proxy HTTP

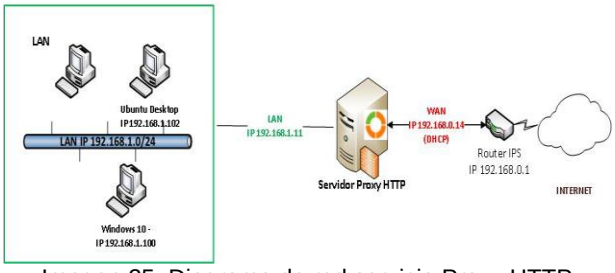

Imagen 25. Diagrama de red servicio Proxy HTTP

La red se compone de un Servidor Zentyal 6.2 con dos tarjetas de red, eth0 con salida a Internet IP 192.168.0.14 y eth1 como Gateway de la red interna con IP 192.168.1.11, por otro lado, en la red interna LAN se compone de un equipo Ubuntu Desktop 18.04 con IP 192.168.1.102/24 y un equipo con Windows 10 en el segmento de red 192.168.1.100/24.

2.3.1 INSTALACIÓN MODULO PROXY HTTP

Al ingresar al servidor Zentyal vía navegador web al link http://192.168.1.11:8443, seleccionar el módulo Proxy HTTP desde el menú seleccionar opción "Seleccionar paquetes a instalar" y el sistema automáticamente informa las dependencias a instalar. Estas dependencias son: Network configuration, Firewall y proxy HTTP: En esta etapa se define los tipos de interfaces de red, su configuración y activación (eth0 Externa con IP 192.168.0.14 y eth1 Interna con IP 192.168.1.11); así como la activación del Firewall (reglas por defecto) y la instalación de los paquetes programas Squid proxy (proxy cache) y Dansguard (filtrado de contenido). Importante resaltar que el proxy de Zentyal únicamente acepta conexiones provenientes de las interfaces de red internas, por tanto, se debe usar una dirección interna en la configuración del navegador.

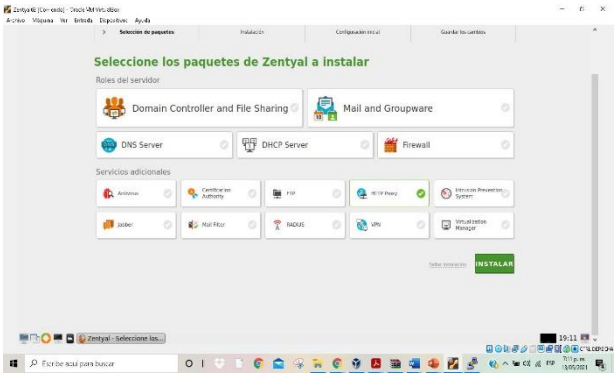

Imagen 26. Instalación modulo Proxy HTTP

2.3.2 OBJETOS DE RED Y SUS MIEMBROS

Importante definir previamente los objetos de red y sus miembros (direcciones IP) para facilitar la creación de reglas de acceso y perfiles de filtrado en el servicio proxy HTTP, los objetos también aplica para cualquier otro servicio como Cortafuegos, DHCP, etc. Para el caso de estudio crear los siguientes objetos de red y sus miembros, así: Objeto Administración con miembro administrador con la IP 192.168.1.11, objeto Cliente_Windows con miembro Windows10 con IP 192.168.1.100 y objeto Cliente_Linux con miembro Ubuntu-cliente con IP 192.168.1.102.

2.3.3 CONFIGURACIÓN PROXY HTTP NO TRANSPARENTE

Para la configuración del servicio Proxy HTTP se debe realizar los siguientes pasos:

Configuración General: Definir el tipo de Proxy, transparente o No transparente (definir No transparente), tamaño cache en MB (100 MB), puerto donde escucha el servicio (default 3128), pro se configura puerto 1230 por requerimiento del ejercicio.

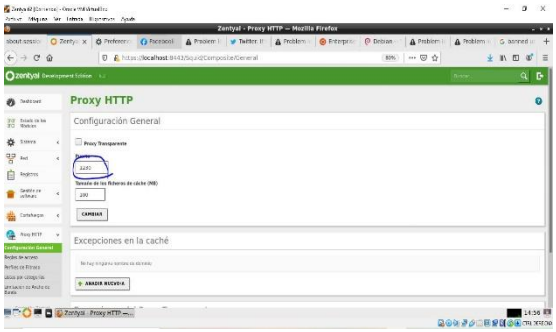

Imagen 27. Tipo de proxy, puerto y memoria cache

Reglas de Acceso: Aquí se define los parámetros de las reglas de acceso. Definir periodo de tiempo de aplicación de la regla (fin de semana, entre semana, horarios), Origen (dirección IP, red interna, objeto de red) y la decisión (permitir, denegar o aplicar perfil de filtrado).

Para el caso de estudio definir tres reglas: La primera periodo tiempo a siempre para el origen objeto de red Cliente-windows y aplicar perfil de filtrado Redes sociales, la segunda regla periodo tiempo a siempre para el origen objeto de red Cliente-Linux y aplicar regla denegar y la tercera regla periodo tiempo a siempre para el origen objeto de red Administración y aplicar perfil de filtrado Listas-Shalla. Importante resaltar que los objetos de red fueron definimos previamente.

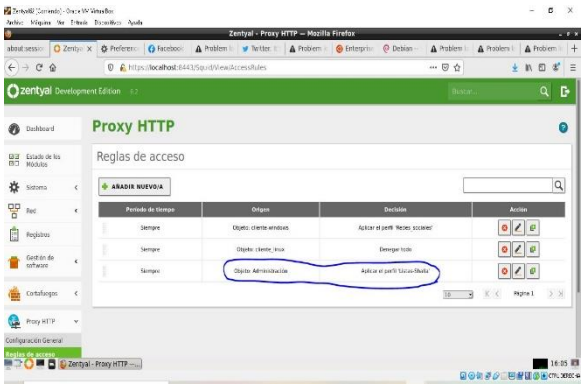

Imagen 28. Reglas de acceso servicio Proxy HTTP

Perfiles de Filtrado: Definir nombre del perfil y su configuración para aplicar el proceso de filtrado. Los parámetros para configurar son: Umbral (desde deshabilitado, permisivo, Medio, Estricto, muy estricto), Reglas de dominios o URL (dominios a aplicar el filtro y la decisión de permitir, o denegar), categorías de dominios (listas negras), Tipos MIME y extensiones de archivos (.bat, .exe, .zip, etc.).

Para el caso de estudio se crean los perfiles Redes_Sociales con umbral estricto y la cual filtra los dominios de las redes sociales Facebook, twitter y YouTube. Un segundo perfil de filtrado llamado Listas-Shalla con umbral estricto la cual filtra dominios por categoría: Bancos, Videos, Hacker, Pornografía, etc.

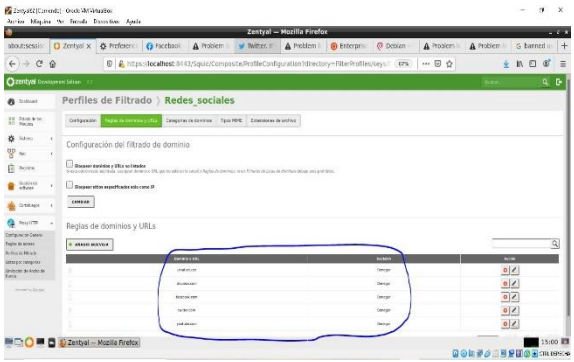

Imagen 29. Reglas de dominios y URLs a filtrar

Listas por Categorías: Listas negras de dominios clasificados por categorías. Por ejemplo, categorías Pornografía, Videos, hackers, bancos, etc. Para el caso de estudio añadir la lista de categorías de dominios Shallalist al servicio Proxy HTTP. Para esto, descargar archivo shallalist.tar.gz desde el sitio http://www.shallalist.de y luego añadir a nuestro proxy.

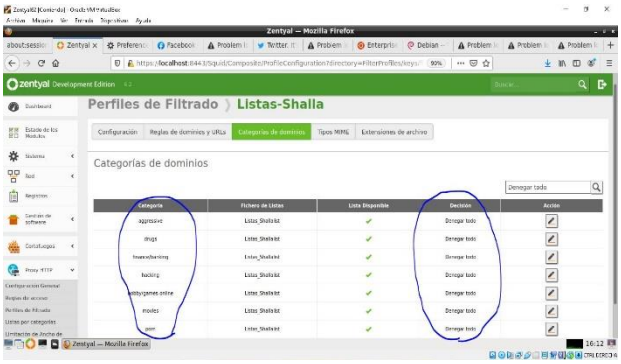

Imagen 30. Perfiles de filtrado Listas-Shalla

2.3.4 PRUEBAS PROXY HTTP NO TRANSPARENTE

Las pruebas del servidor proxy se realizan desde la red interna LAN (clientes Windos10 y Ubuntu Desktop). Antes de realizar las pruebas de filtrado en el navegador web del cliente (Chrome, Mozilla Firefox, etc.) es necesario configurar por cada protocolo (HTTP o HTTPS) la dirección IP y puerto del servidor proxy Zentyal. En el caso de estudio ingresar la IP del servidor Zentyal 192.168.1.11 y el puerto 1230, de tal forma que al realizar la navegación a un dominio web, la solicitud sea procesada y validada en el servidor proxy acorde a las reglas y filtros definidos anteriormente.

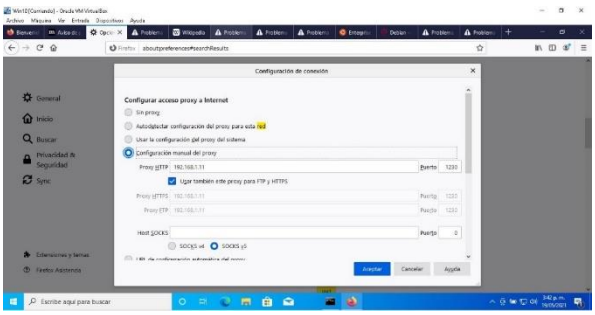

Imagen 31. Configuración manual del proxy en navegador Mozilla firefox

Una vez configurados los navegadores iniciar las pruebas ingresando a varias páginas web desde los objetos de red configurados.

Inicialmente desde la maquia Windows 10, donde tiene configurado el perfil Redes-Sociales, ingresar a la red social Facebook https://www.facebook.com y se observa que aparece el mensaje de bloqueo por el proxy Mensaje “El servidor proxy está rechazando la conexión”, evidenciando la funcionalidad del servicio Proxy HTTP no transparente

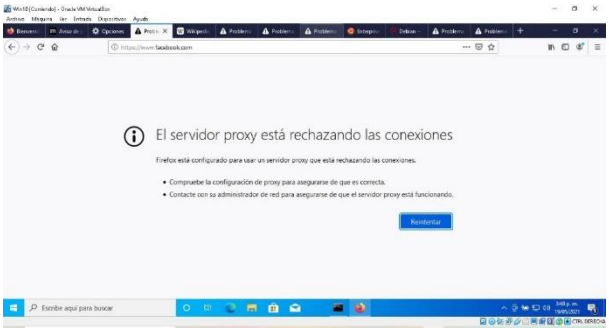

Imagen32. Servidor proxy rechaza conexión en navegador Mozilla Firefox de la maquina Windows 10

Ahora desde la maquina Ubuntu-desktop, donde tiene configurado la regla de acceso DENEGAR TODO, ingresar al sitio https://www.youtube.com, se observa mensaje de bloqueo por el proxy, mensaje "El servidor proxy está rechazando la conexión, evidenciando la funcionalidad del servicio Proxy HTTP no transparente

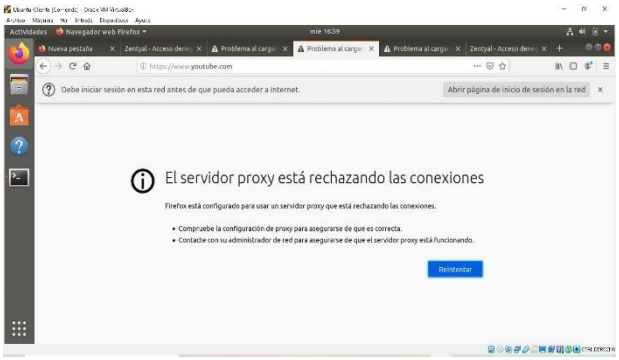

Imagen 33. Servidor proxy rechaza conexión en navegador Mozilla Firefox de la maquina Ubuntu Desktop 18.04

2.4 TEMÁTICA 3: CORTAFUEGOS

Temática desarrollada por el estudiante Miguel Ángel Barahona Ordoñez.

Una vez instalado y configurado Zentyal, se debe instalar dos módulos que se necesitan para dar solución a la problemática. Para la actividad se requiere instalar el servicio cortafuegos (Firewall), para poder tener comunicación entre el host (cliente) y el servidor como garantizar que el tráfico que genera el host (cliente) pase por el cortafuegos se instala el servicio DHCP Server.

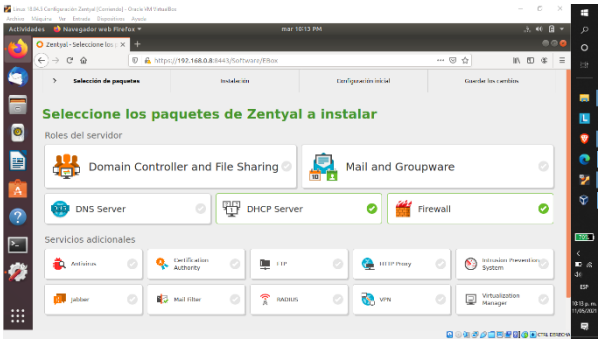

Imagen 34. Instalación paquete Firewall y DHCP Server

Instalado los servicios requeridos, se pasa a la opción de las interfaces, la primera interfaz (eth0) es de del método DHCP y se dejará como red externa de tipo WAN el cual tendrá acceso a internet. Frente a la segunda interfaz (eth1) su método será estático y se le asigna la dirección de red 192.168.0.8/24, esta interfaz trabajará de forma interna (Zona verde).

Imagen 35. Configuración de interfaces Zentyal.

Una vez se configure las interfaces se aplica los módulos (Red, Cortafuegos y DHCP) sobre el servidor para que se instale con sus dependencias necesarias para su funcionamiento. Se pasa a la pestaña DHCP server y se configura un rango de direcciones IP a entregar a los equipos hosts (cliente).

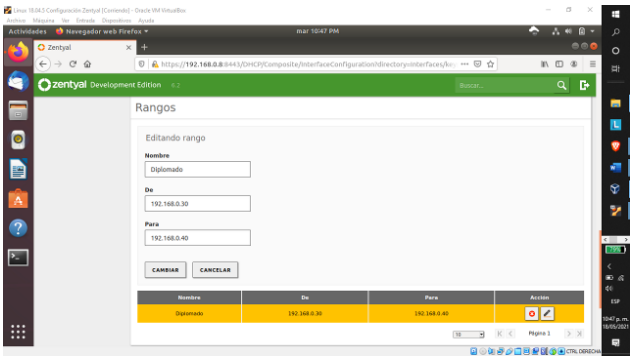

Imagen 36. Configuración de rango de direccionamiento servidor DHCP Server.

Cuando se aplica los cambios sobre el servidor, se enciende la maquina host (cliente) de tipo *Ubuntu-desktop 18.04*, esta máquina solo tendrá un adaptador por red interna. Se pasa a la opción de Red una vez se encienda, se crea un nuevo perfil llamado *Diplomado* y se define la opción de buscar la IP y el DNS de forma automática.

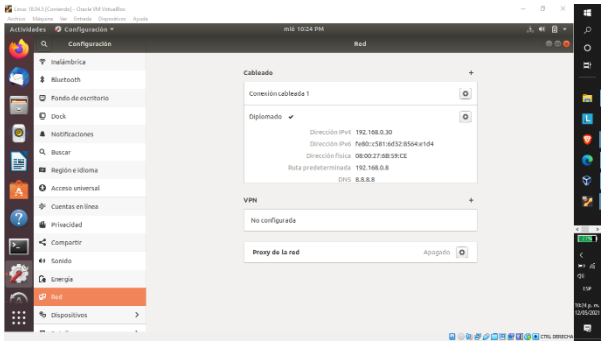

Imagen 37. Creación de perfil y búsqueda de IP de forma automática.

Para comprobar que el servidor asigno una dirección de red al host (Cliente) se revisa la MAC he IP desde el host (cliente) abriendo la terminal e ingresando el comando *ifconfig* se compara desde el dashboard de Zentyal (Servidor).

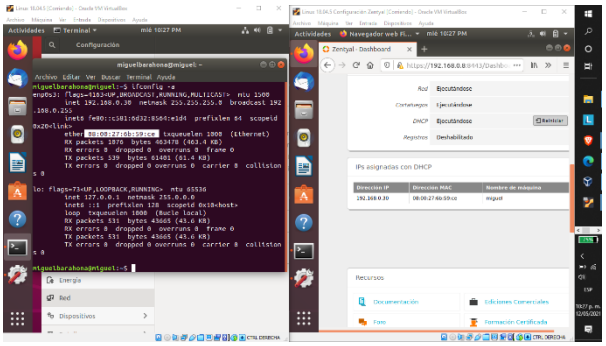

Imagen 38. Validación asignación de IP desde el servidor al host (cliente).

Se valida que el host (cliente) pueda navegar por internet.

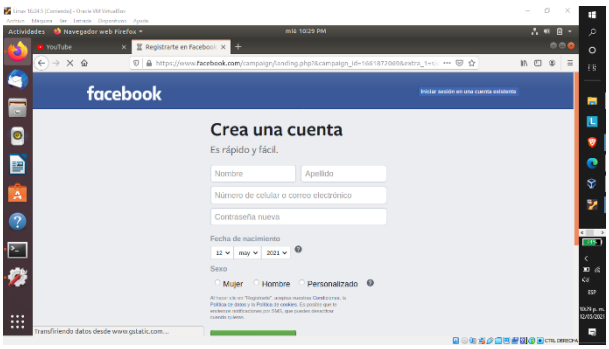

Imagen 39. Validación de navegación desde el host (cliente).

Tabla 1. CIDR a bloquear

Sitio o Portal	CIDR
Netflix	3.208.0.0/12 54.144.0.0/12 54.160.0.0/11 54.192.0.0/12 54.208.0.0/13 54.216.0.0/14 54.220.0.0/15 3.224.0.0/12
Facebook	157.240.0.0/16
Telegram	149.154.0.0/16

Para obtener el CIDR (enrutamiento entre dominios sin clases) de cada sitio se requiere obtener las direcciones IP que contiene los sitios, por lo cual a cada sitio desde la terminal del host (cliente) se ejecuta el siguiente comando *nslookup "dominio",* este caso de ejemplo con *Netflix → nslookup www.netflix.com*.

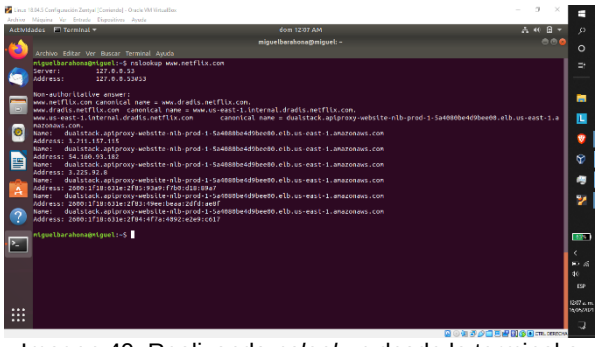

Imagen 40. Realizando *nslookup* desde la terminal a *Netflix*.

Al obtener las direcciones, se utiliza la siguiente página llamada *Whois* donde se sacará el CDIR con su respectivo prefijo de red, con solo ingresar la IP de cada sitio.

***Nota**: Este paso se realiza para cada uno de los sitios.*

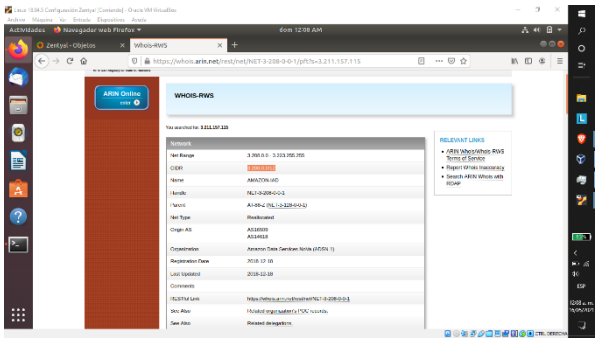

Imagen 41. Obteniendo el CIDR del sitio *Netflix* desde la IP.

Al obtener el CIDR de cada sitio se crea un objeto a cada sitio desde la opción *Red → Objetos*.

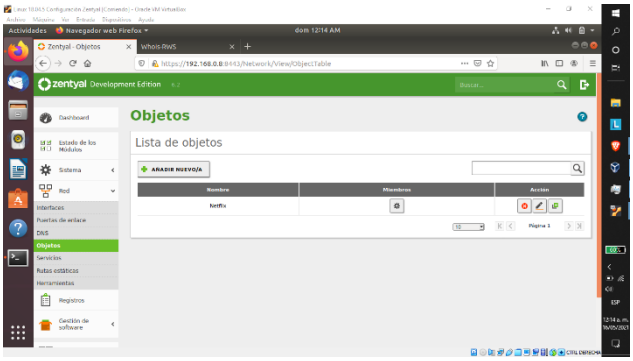

Imagen 42. Se crea el objeto llamado *Netflix*.

Ahora se crea los miembros necesarios para cada sitio, en este caso *Netflix* como son varias direcciones se crean varios miembros, sobre el mismo objeto.

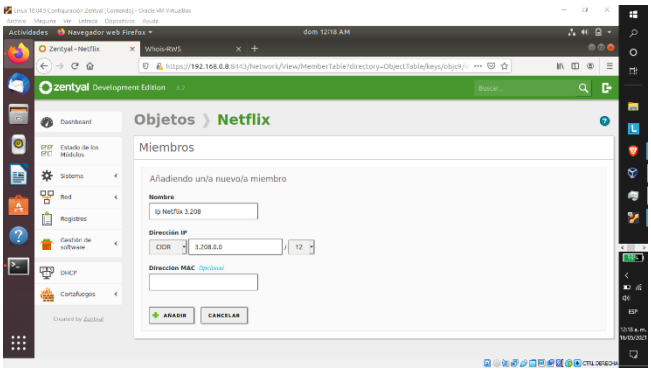

Imagen 43. Se crea un miembro para el sitio de *Netflix*.

Una vez se crea los objetos y miembros necesarios de cada objeto, Se pasa a la opción *Cortafuegos → Filtrado de paquetes,* en donde se dirige a la opción "*Reglas de filtrado para las redes internas*" ya que el equipo host (cliente) está conectado por red interna.

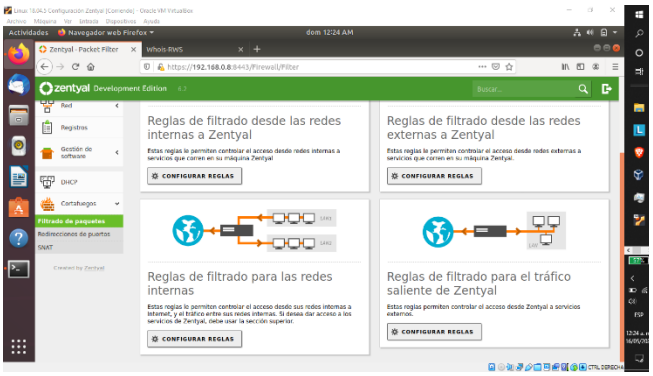

Imagen 44. Opción → "*Reglas de filtrado para las redes internas*".

Se crea una nueva regla para *Netflix* de forma personalizada, este mismo paso se realiza para los demás sitios.

Las reglas se crearán de la siguiente forma:
Decisión: Denegar.

Origen: Cualquiera (Petición desde cualquier equipo que esté conectado sobre la red interna).
Destino: Se selecciona. *Objeto destino → Netflix*
Servicio: Cualquiera (Ejemplo: TCP, HTTP, HTTPS, etc.).
Descripción: Bloqueo y Nombre del sitio. *Ejemplo: Bloqueo Netflix*.

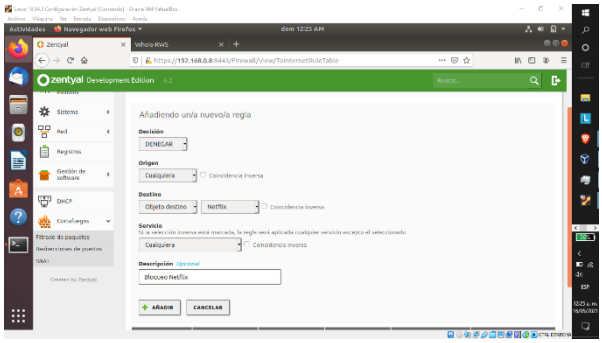

Imagen 45. Se crea una regla llamada *Netflix*.

Al crear las reglas para cada uno de los sitios con base en la tabla, se ubica sobre la maquina host (cliente) y se intenta navegar desde el navegador de Firefox y realizar ping, al sitio de *Netflix*.

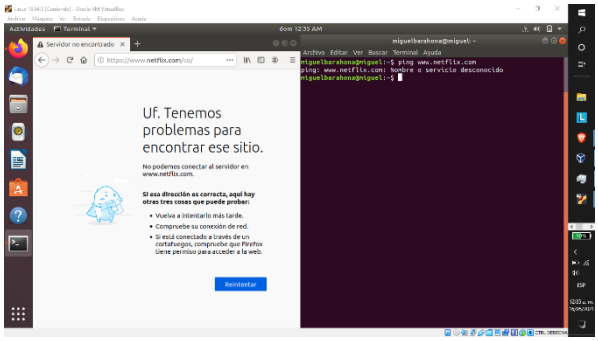

Imagen 46. Intentando ingresar desde el navegador y realizando ping al dominio de *Netflix*.

Como se evidencia la navegación web como las peticiones desde la terminal se encuentran bloqueadas, ya que el cortafuego de Zentyal está ejecutando las reglas de filtrado web sobre el host (cliente).

2.5 TEMÁTICA 4: FILE SERVER Y PRINT SERVER

Temática desarrollada por el estudiante Omar Edilson Infante Peña

En el presente apartado se presenta la configuración de controlador de dominio y un print server, con la posibilidad de gestión usuario y grupos para habilitar acceso a los recursos que se encuentran compartidos; el proceso inicia instalando Zentyal, en el entorno gráfico se debe configurar una interface de red interna para el acceso remoto al servidor y poder aplicar el DNS, DHCP y función del servidor como Gateway desde la interface

externa que se conectara como WAN y puente en virtual Box.

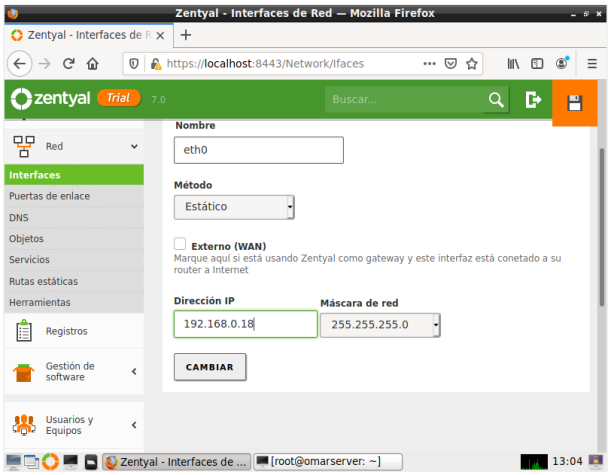

Imagen 47. Configuración de interfaces de red.

Aquí elegimos los módulos o paquetes a actualizar, en este caso para conocer cada una de las funciones de los módulos se recomienda instalar 1 a 1 el DNS, DHCP y Red; para finalmente instalar todo el rol de Controlador de dominio y Compartición de archivos.

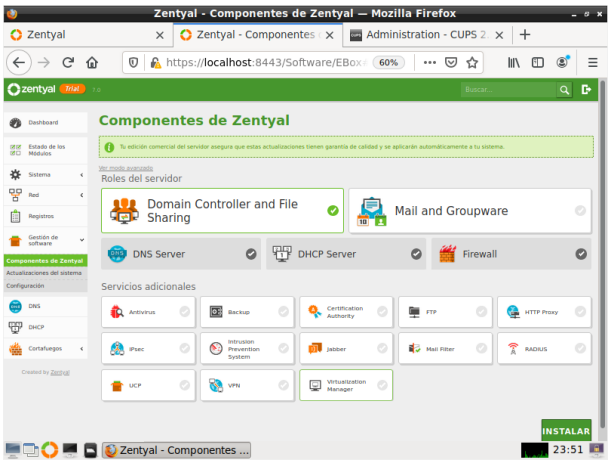

Imagen 48. Instalación módulos Domain Controler and file sharing.

Instalado los módulos requeridos, se deben habilitar los usuario que van a funcionar en este caso con el dominio hercules.local; para este ejemplo se crearon dos usuarios administrador y el empleado.

Imagen 49. Configuración de usuario de dominio.

Desde la opción de compartición de ficheros se añade un nuevo directorio llamado PrintServer encontrado en la ruta definida por Zentyal; después de creada la carpeta se genera el control de acceso con permisos de lectura y escritura para el usuario oinfante que es el que tiene el rol de empleado.

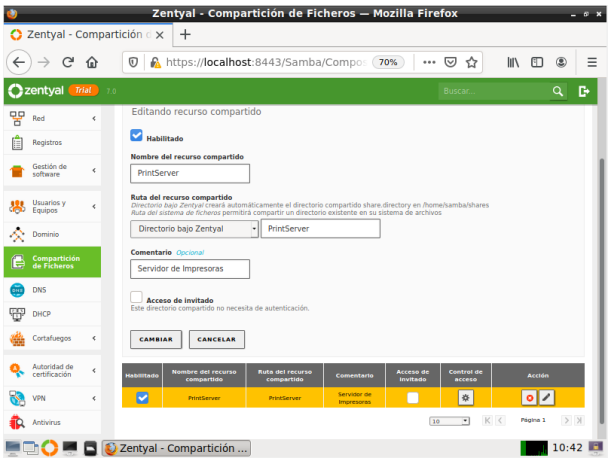

Imagen 50. Compartición de ficheros y control de acceso

cada cambio que se realice sobre el servidor se debe ir guardando para que no genere conflicto y no afecte los servicios prestados. En la maquina cliente de Ubuntu-desktop, para unir la maquina al active directory se debe realizar la descarga de la aplicación pbis-open e instalación según arquitectura del computador.

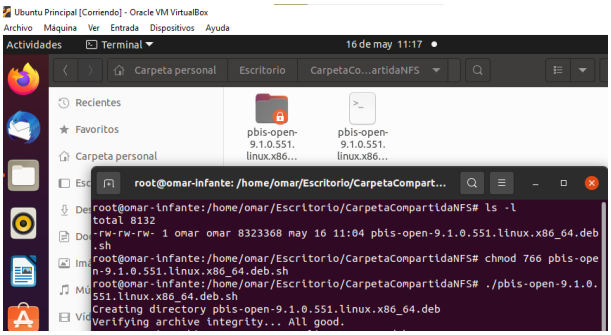

Imagen 51. Unión de Active Directory desde línea de comandos.

En el Ubuntu Desktop se debe instalar el Paquete cliente de samba, posteriormente se debe agregar el usuario configurado para acceso de dominio oinfante@hercules.local; Se procede a montar la carpeta compartida en el Cliente ingresando las credenciales de registradas en Zentyal, el montaje de la unidad SMB remota para el usuario oinfante se realiza con usuario local.

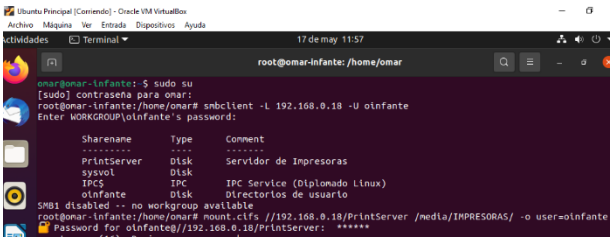

Imagen 52. Montaje de carpeta compartida.

Como se aprecia en la carpeta /media/IMPRESORAS está montado el recurso compartido de PrintServer.

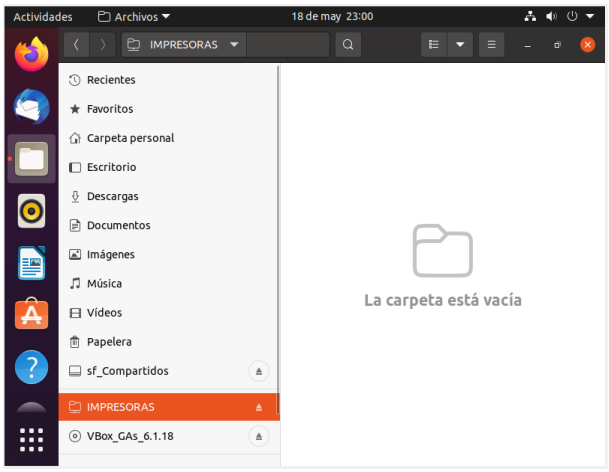

Imagen 53. Validación de carpeta Compartida

A continuación, se describe el proceso para configurar el print server, teniendo que se continua el uso de controlador de dominio por medio de samba. Se instala el paquete cups en el servidor Zentyal Con el comando sudo apt-get install cups.

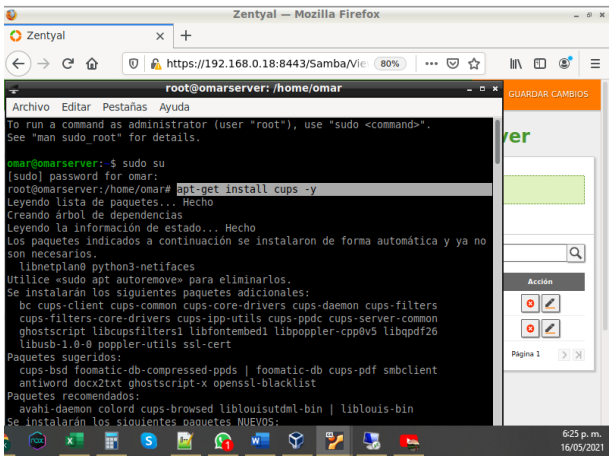

Imagen 54. Instalando controlador para impresiones.

Luego de ello se configura el nombre de la impresora virtual para hacer las pruebas.

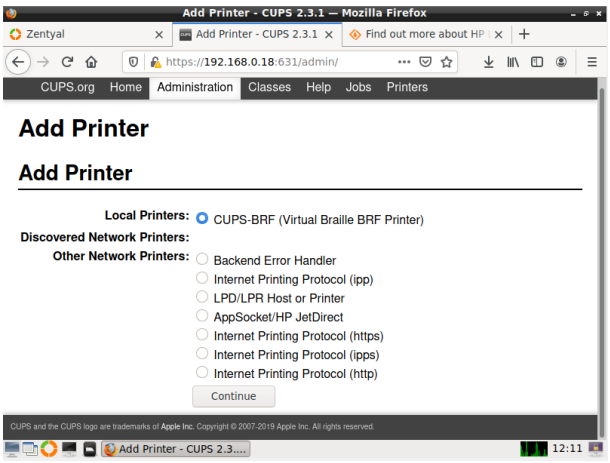

Imagen 55. Impresora virtual CUPS

Se procede a agregar el código para el archivo smb.conf para indicar al servidor Zentyal que se deben compartir todas las impresoras por samba, cuando la impresora este configurada, Una vez vayamos a imprimir se abrirá una ventana de notificación en el que se debe ingresar las credenciales, es importante aclarar que el reinicio del servidor Sentyal versión 7.1 genera que el archivo smb.conf vuelva a sus valores por defecto, de igual manera según la documentación consulta indica que el print server estuvo disponible hasta la versión 4.0

2.6 TEMÁTICA 5: VPN

2.6.1 CONFIGURACIÓN EN SERVIDOR ZENTYAL

Producto esperado: Implementación y configuración detallada de la creación de una VPN que permita establecer un túnel privado de comunicación con una estación de trabajo GNU/Linux. Se debe evidenciar el ingreso a algún contenido o aplicación de la estación de trabajo.

Después de la instalación de Zentyal se carga el sistema y automáticamente se abre el login de autenticación de usuario para configurar el servidor. Al realizar la autenticación, se emperezará por la configuración inicial de Zentyal, seleccionando el servicio solicitado, en este caso VPN. Al continuar, se mostrarán los paquetes que se instalarán en el servidor, los cuales son Network Configuration, Firewall, Certification Authority y VPN.

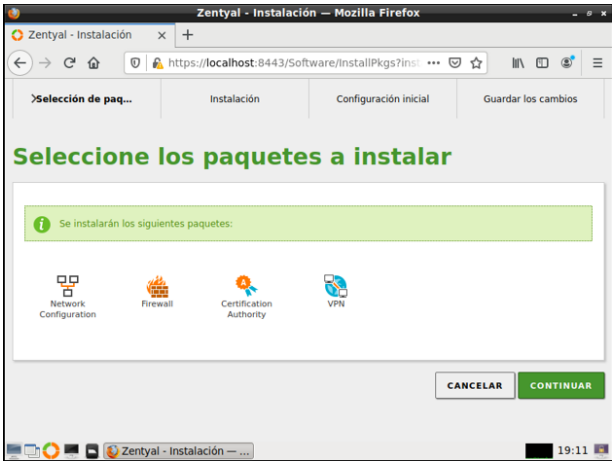

Imagen 56. Paquetes de instación para vpn

Una vez descargado e instalados los paquetes anteriores, se procede a realizar la configuración de las interfaces. Siguiente a ello, se guardará la configuración y se permitirá iniciar la Dashboard.

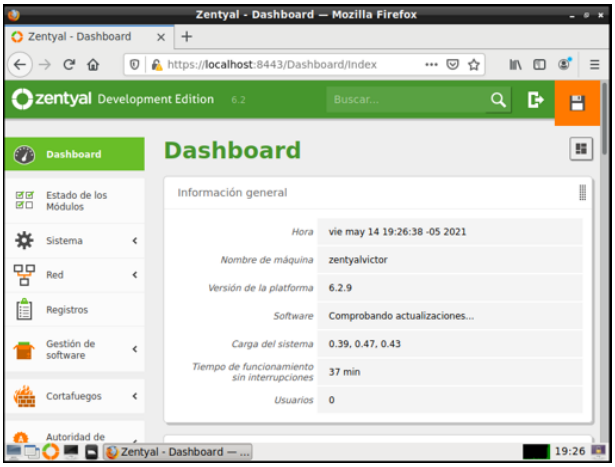

Imagen 57. Dashboard.

Hecho esto, se procede a abrir el apartado de Autoridad de Certificación/General, y una vez aquí se creará un certificado para que se permita la implementación de un nuevo servidor VPN. Se añadirá inicialmente una nueva Autoridad de certificación, se le asigna un nombre y los días para expirar.

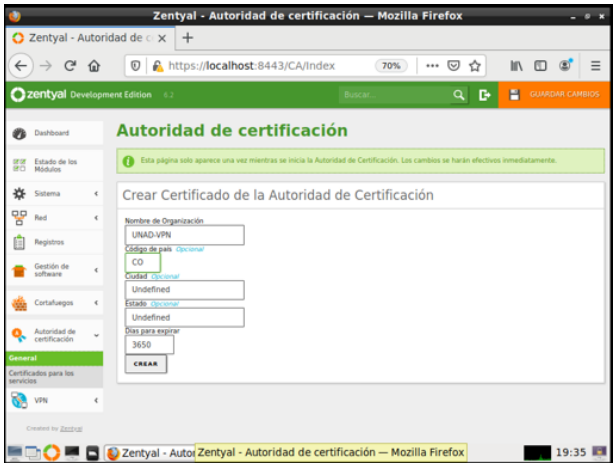

Imagen 58. Creando autoridad de certificación.

Después, carga la ventana donde muestra el Certificado de Autoridad en la parte inferior y muestra la opción de expedir un nuevo certificado. Se debe expedir uno con un nombre y días para la expiración del mismo. Este certificado será para el funcionamiento del servidor VPN.

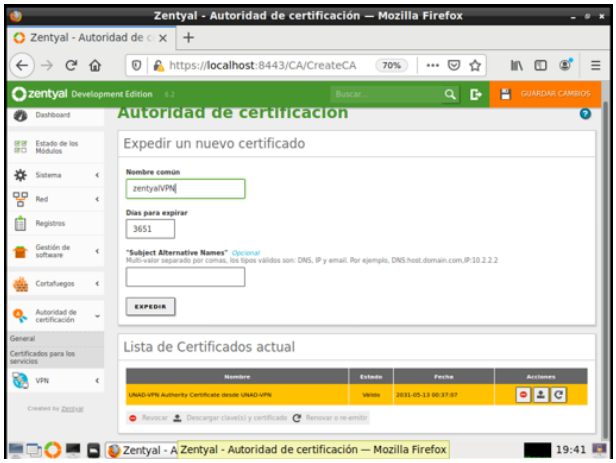

Imagen 59. Expedición de certificado para servidor VPN.

Una vez expedido el certificado, se habilita la posibilidad de añadir un nuevo servidor VPN en el apartado VPN/Servidores. Una vez se selecciona la opción de añadir, se le asigna un nombre al servidor VPN y nuevamente se selecciona añadir.

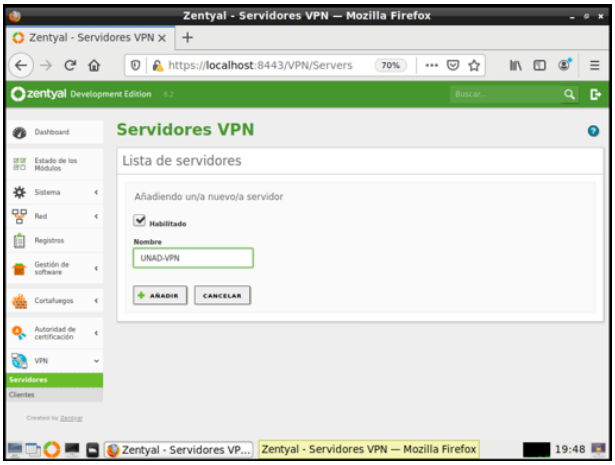

Imagen 60. Añadiendo servidor VPN

Una vez añadido, se selecciona la opción de configuración del servidor donde se configurarán los parámetros del mismo, asignándole un puerto UDP, dirección del VPN (por defecto suele ser 192.168.160.0/24), se selecciona el certificado anteriormente expedido y se configuran los demás parámetros.

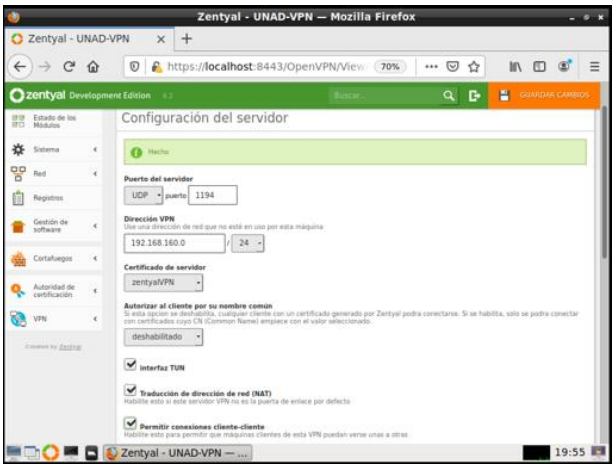

Imagen 61. Parámetros de configuración del servidor VPN

Después de configurar se selecciona el botón de cambiar y se guardan los cambios. Después se continua por expedir otro certificado, en esta ocasión, para el cliente.

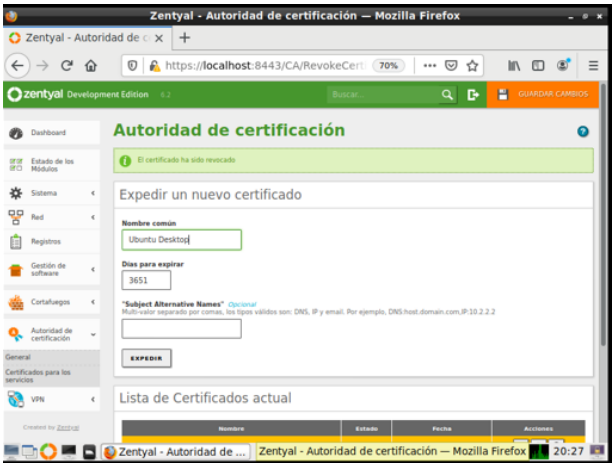

Imagen 62. Expedición de certificado para Cliente.

Después de expedido el certificado del cliente, nuevamente en VPN/Servidores, se selecciona la opción “Descargar paquete de configuración de cliente”, esto permitirá poder expedir un paquete de configuraciones para que el cliente. Una vez se selecciona esta opción, se cara la ventana y se debe configurar de qué tipo el el cliente, se selecciona el certificado del cliente y se selecciona la dirección IP para el servidor VPN, esta debe ser una IP estática, las demás opciones son opcionales.

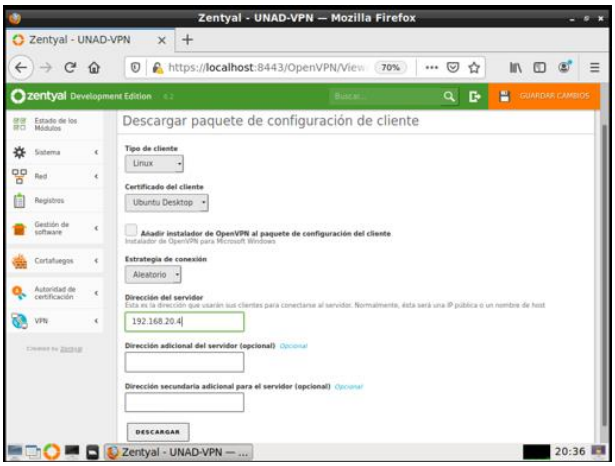

Imagen 63. Paquete de configuración del cliente.

Una vez configurado lo anterior, se da en botón de descargar y se guarda el paquete de la configuración. Este paquete le permite al cliente, en el momento de añadir una VPN usarlo parala configuración de manera automática.

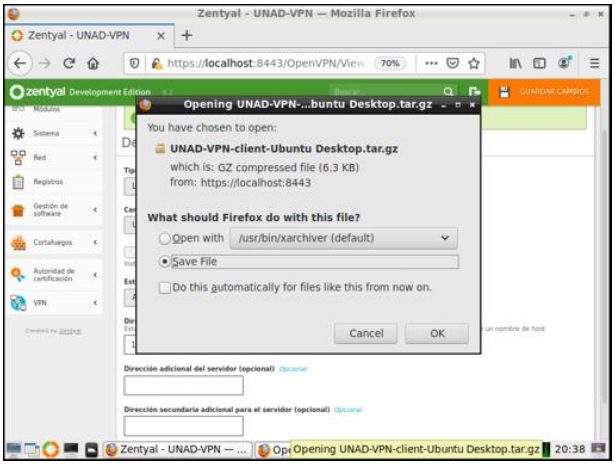

Imagen 64. Descarga del paquete de configuración del cliente

2.6.2 CONFIGURACIÓN EN CLIENTE

Una vez en el cliente, en la configuración de red, se dirige al apartado de VPN, y se selecciona la opción para añadir una nueva conexión VPN. Una vez se hace el paso anterior, se selecciona el tipo en que se a configurar la conexión. Si no es posible mover el paquete de configuración para el cliente que se descargó anteriormente, se procede a configurar de la siguiente manera. Se selecciona el Protocolo de túnel punto a punto (PPTP). Una vez hecho esto, se le asigna un nombre a la conexión y se le agrega la pasarela, que es la dirección IP estática que se agregó en la configuración. Después se selecciona la configuración avanzada.

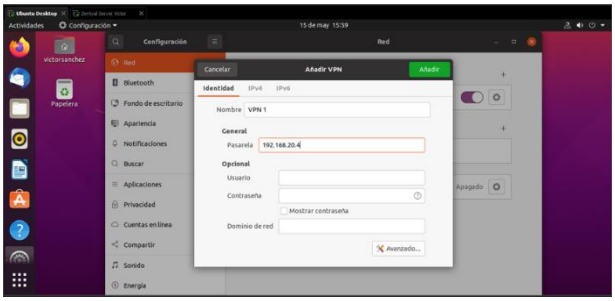

Imagen 65. Añadiendo conexión VPN

Una vez en configuración avanzada se selecciona la opción Usar cifrado punto a punto (MPPE). Clic en aceptar y luego en añadir para culminar la agregación del VPN.

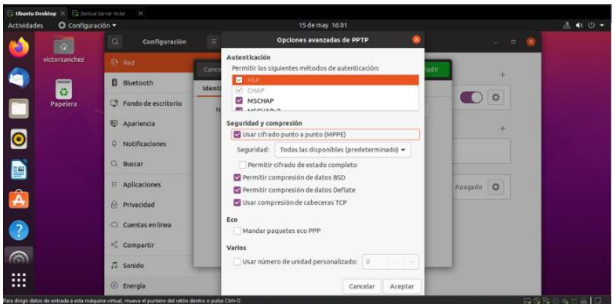

Imagen 66. Configuración avanzada

Después de añadida la conexión VPN, ya se puede usar. Se podrá habilitar desde configuración de red o desde el menú de opciones en la parte superior derecha del cliente, VPN y conectar. Al mismo tiempo se deberá autenticar para que permita la conexión.

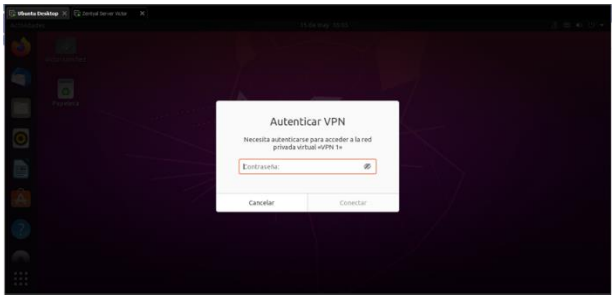

Imagen 67. Autenticación para habilitar conexión VPN

Una forma de mostrar que el servidor VPN se está ejecutando, puede ser en la Dashboard del servidor Zentyal donde se muestra un widget de los Demonios OpenVPN.

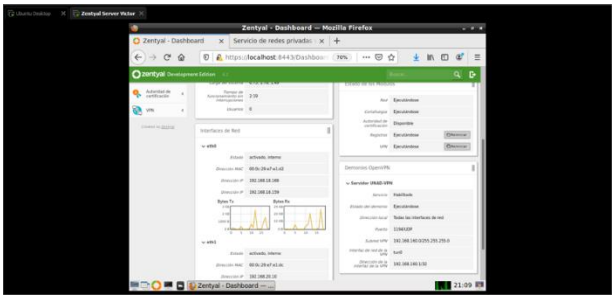

Imagen 68. Información de demonios OpenVPN

3 CONCLUSIONES

Zentyal ofrece una gran variedad de herramientas para administrar una red LAN, proxy, firewall, dominio, DHCP, entre otras soluciones tecnológicas que son suficientes para el sector empresarial.

Con Zentyal permite configurar el paquete DHCP server, para asignar una IP a los equipos host (cliente) por medio de la red interna y una vez se asigne la Ip, poder controlar el tráfico de red y colocar las reglas desde el paquete de cortafuegos (firewall) necesarios para bloquear sitios web.

Los servicios de acceso al directorio se gestionan por el protocolo ligero de acceso a directorios LDAP con una gestión de permisos centralizada desde el servidor; de esta forma, los usuarios pueden autenticarse de manera remota a los ficheros e incluso la posibilidad acceso a impresión. La posibilidad de aplicar permisos de acceso y modificación por usuario facilita de gran manera la gestión para las empresas ya se puede definir una directiva de control sobre documentos, impresoras y programas de forma automática.

Los servicios de proxy HTTP permite obtener una reducción del uso del ancho de banda, mejora los tiempos de respuesta en las consultas a sitios web, filtración de contenidos, control el acceso a sitios web, aplicación de listas negras a dominios por categorías y fortalecimiento de la seguridad de la red mediante la aplicación de reglas y filtros del tráfico de información.

La configuración de una VPN en Zentyal permite crear conexiones seguras privadas a una red local, de manera que el acceso a la información y recursos es seguro y fiable, sin riesgo de filtraciones ni acceso no autorizado.

4 REFERENCIAS

[1] Zentyal Community. (2015) Instalación Zentyal 6.2 Disponible en: https://doc.zentyal.org/6.2/es/installation.html

[2] CANONICAL. (Sin fecha). Netplan configuration examples [En línea]. Disponible en: https://netplan.io/examples/.

[3] Zentyal Community. (Sin fecha). Servicio de configuración de red (DHCP) [En línea]. Disponible en : https://doc.zentyal.org/6.2/es/dhcp.html.

[4] Zentyal Community. (Sin fecha). Instalación [En línea]. Disponible en: https://doc.zentyal.org/es/installation.html#.

[5] Zentyal Community. (Sin fecha). Cortafuegos [En línea]. Disponible en: https://doc.zentyal.org/es/firewall.html.

[6] J. Gómez (2014, abril 30). Zentyal - Instalar y configurar DHCP Server [En línea]. Disponible en: https://www.youtube.com/watch?v=H5lhAKOH5LM.

[7] Jherz (2020, agosto 03). Configuración de firewall para denegar páginas en zentyal parte 2 [En línea]. Disponible en: https://www.youtube.com/watch?v=jZvjWnTzTbk.

[8] D. Guide. IONOS (2019, abril 04). CIDR: el classles inter-domain routing en detalle [En línea]. Disponible en: https://www.ionos.es/digitalguide/servidores/know-how/classless-inter-domain-routing/.

[9] Shalla, «http://www.shallalist.de/,» s.f. [En línea]. [Último acceso: mayo 2021].

[10] Zentyal, «https://doc.zentyal.org/6.2/es/index.html,» s.f. [En línea]. [Último acceso: mayo 2021].

[11] Zentyal Community. (2015) Servicio de redes privadas virtuales (VPN) con OpenVPN Disponible en: https://doc.zentyal.org/6.2/es/vpn.html#configuracion-de-un-servidor-openvpn-con-zentyal