Curso Profundización en Linux
Implementación de servicios en plataforma Zentyal Server en el sistema GNU/Linux.

Leonardo Celeita Cifuentes, Yeison Yair Córdoba Martínez, Álvaro Stivens Moreno, Mayra Alejandra Moreno Borrero, Andry Jessica Toro Villa.

Universidad Nacional Abierta y a Distancia UNAD
Colombia
leonardo.celeita@gmail.com
yeisonyairc@gmail.com
stivens128@gmail.com
maleja06240@hotmail.com
andryjessica@hotmail.com

***Abstract*— En este documento se muestra el proceso de instalación y configuración de cada uno de los servicios proporcionados por el servidor Zentyal, además se gestiona los diferentes servicios para comunicar con los clientes y prestar soluciones de seguridad de acuerdo a las necesidades requeridas.**

Palabras claves – zentyal, configuración, instalación, DHCP, DNS, Proxy, VPN, File.

I. INTRODUCCIÓN

El sistema GNU/Linux es uno de los sistemas operativos más utilizados para la implementación y configuración de servidores a nivel mundial, por su seguridad y robustez a la hora de implementar los servicios, proporciona una buena administración y control, lo que lo hace ideal para el manejo de la seguridad informática, infraestructura de red, puertas de enlace, servidor de oficina y comunicaciones e implementación de servicios.

Una de las distribuciones utilizadas como servidor de pequeñas y medianas empresas para la implementación de servicios en infraestructura IT intranet y extranet es Zentyal Server Linux Small Bussines, que mediante una GUI fácil e intuitiva, permite administrar y gestionar diferentes servicios Web, como son DHCP, DNS, VPN, Proxy, Cortafuegos (Firewall), servidor de archivos e impresión, además presenta compatibilidad con Active Directory de Windows, ayudando a muchas empresas a realizar diferentes tareas en una plataforma tecnológica de software libre.

II. DESARROLLO EN EL SISTEMA ZENTYAL SERVER

En el documento se muestra la instalación del sistema operativo Zentyal Server 6.0 y la instalación y configuración de los servicios ya mencionados, la forma de administrar, controlar y limitar dependiendo de las necesidades y de acuerdo a la infraestructura red, proveedor de internet y número de nodos que maneje la empresa.

A. Configuración

Después de la instalación el sistema se reinicia, y se muestra el sistema arrancando y acabando de instalar paquetes de segunda fase, al cargar, se muestra el escritorio, para utilizarse.

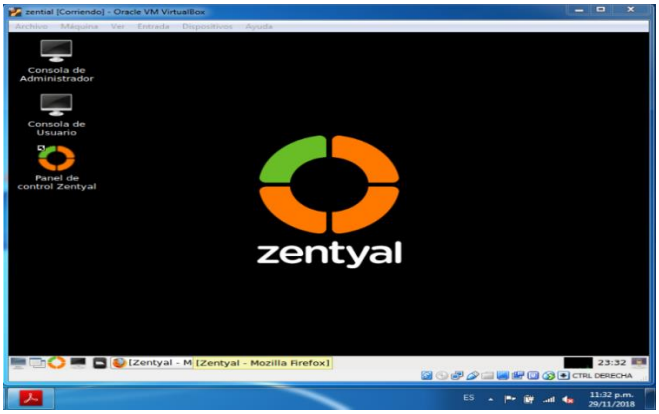


Imagen 1. Escritorio Zentyal.

Seleccionar en el escritorio el panel de control Zentyal, se abre el navegador Firefox en la siguiente ruta https://localhost:8443/software/welcome/, con un formulario de inicio de sesión y contraseña, que son los mismos que ingreso al instalar el sistema.

Imagen 2. Zentyal, inicio sesión.

Se muestra una ventana con las funciones y servicios disponibles que pueden ser instalados en el servidor, se seleccionan de acuerdo a la temática y Zentyal hace una pre configuración, adaptándola según los requerimientos de cada usuario y termina seleccionando los paquetes faltantes, se marca en verde los que desea, luego le da en instalar.

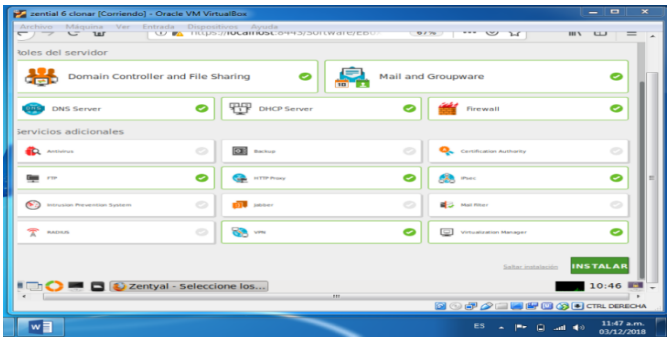


Imagen 3. Menú de opciones de servicios a instalar.

El adaptador 1, enp0s3 que es la red externa (WAN), se escoge el método automático DHCP, toma una dirección IP que le da el router.

En el adaptador Enp0s8 es la red interna, se escoge el método estático y se le ingresa una dirección IP, la cual va a quedar el servidor.

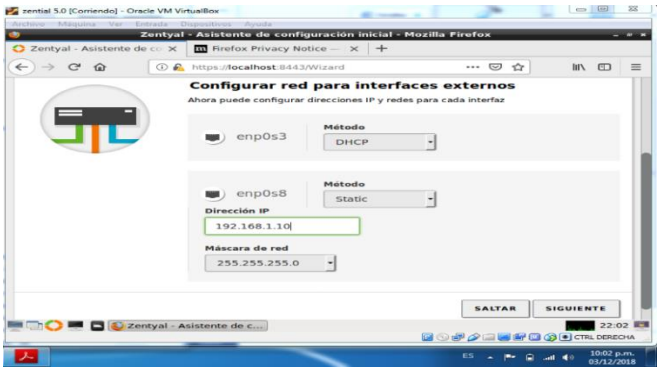


Imagen 4. Interfaces externos e internos.

Después de configurar sigue el proceso instalación de los módulos de servicios, se muestra que la instalación fue completada y se visualiza el Dashboard del Zentyal Server.

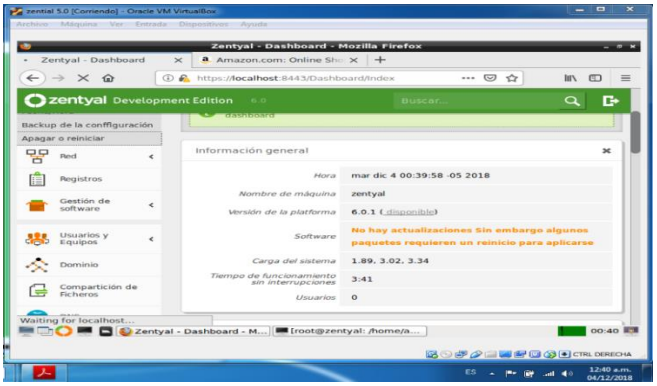


Imagen 5. Escritorio de Zentyal (Dashboard).

III. TEMATICAS

TABLA I

Temática	servicios	Integrante
1	DHCP Server, DNS Server y Controlador de Dominio	Álvaro Stivens Moreno
2	Proxy no transparente	Andry Jessica Toro
3	Cortafuegos	Mayra Alejandra Moreno
4	File Server y Print Server	Yeison Yair Cordoba
5	VPN	Leonardo Celeita

1. DHCP Server, DNS Server y Controlador de Dominio.

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.

Elegimos los siguientes paquetes, DNS Server, DHCP Server y Domain Controller and File Sharing, automáticamente Zentyal ajusta los paquetes requeridos y damos en instalar:

Imagen 6. Inhalación paquetes Zentyal.

Vemos los paquetes seleccionados y los agregados por el servidor, damos en continuar:

Imagen 7. Paquetes seleccionados.

Comienza el proceso de instalación y esperamos a que se complete el 100%, elegimos la configuración de las tarjetas de red:

Imagen 8. Configuración tarjeta Zentyal.

Definimos el rango de dirección IP de la tarjeta usamos el rango de IP de nuestro router:

Imagen 9. Configuración tarjeta de red.

Nos pregunta el tipo de servidor que vamos a trabajar stand-alone y nos proporciona un nombre por defecto:

Imagen 10. Nombre del servidor.

Damos en finalizar esperamos que aplique los cambios y debemos reiniciar el servidor, al reiniciar podremos ver una imagen del dashboard:

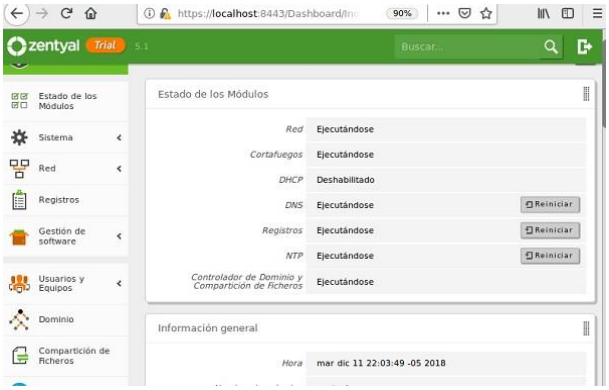


Imagen 11. Dashboard Zentyal, servicios ejecutándose.

Configuración servidor DHCP, damos clic en el icono para completar la configuración, nos muestra una advertencia y como se observó en el dashboard el modulo esta desactivado antes de configurar se debe activar:

Imagen 12. Configuración DHCP.

En estado de los módulos activamos el DHCP y guardamos los cambios, vamos nuevamente a DHCP y configuramos la tarjeta de red:

Imagen 13. Configuración tarjeta de red DHCP.

Después configuramos los rangos en DHCP:

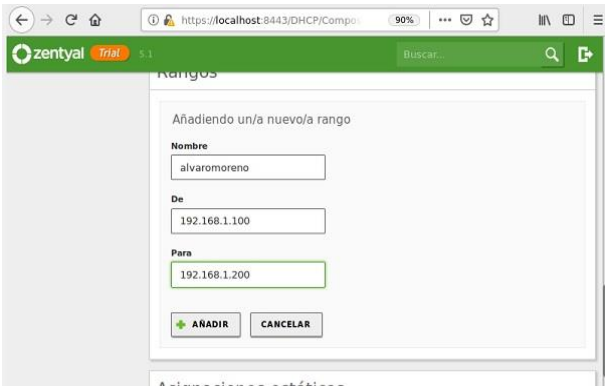


Imagen 14. Configuración rangos DHCP.

Evidencia uso servidor DHCP en Ubuntu desktop y el ingreso en la dashboard del Zentyal de la maquina:

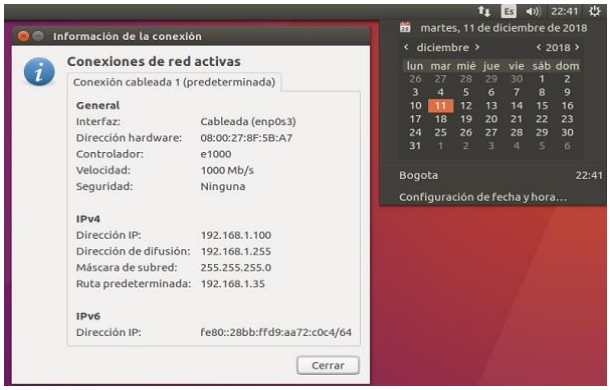


Imagen 15. Evidencia Ubuntu desktop IP dada por el servidor DHCP Zentyal.

Zentyal DHCP funcionado:

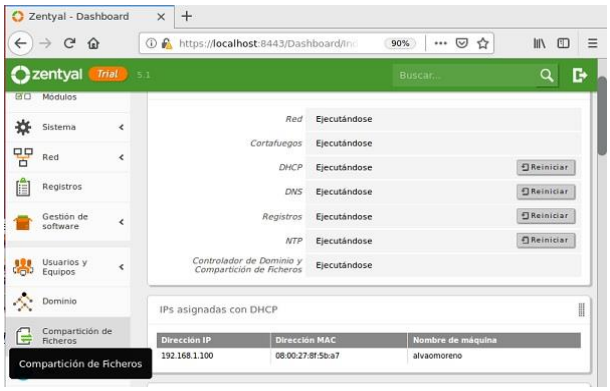


Imagen 16. Evidencia Zentyal, maquina Ubuntu conectada.

Configuración servidor DNS Zentyal, este procedimiento basta con activar el módulo DNS y en las configuraciones que viene por defecto en el servidor Zentyal:

Imagen 17. Configuración DNS Zentyal

Después vamos a DHCP y donde dice servidor de nombre primario seleccionamos DNS local de Zentyal:

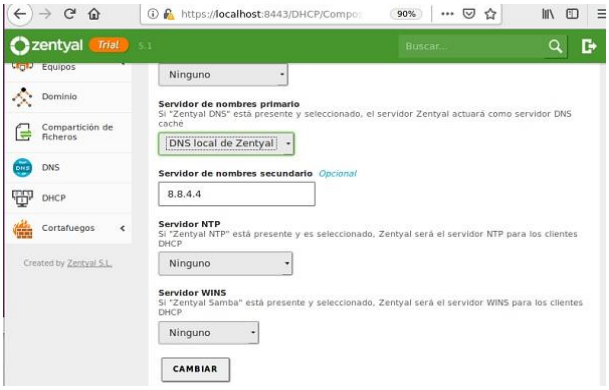


Imagen 18. Configuración DHCP y DNS.

Evidenciamos el uso de los DNS en el Ubuntu Desktop:

Imagen 19. Evidencia uso de los DNS.

El dominio quedo habilitado desde el comienzo de la instalación, solo resta crear los nuevos usuarios o grupos de usuarios para ello vamos al icono usuarios y creamos uno nuevo:

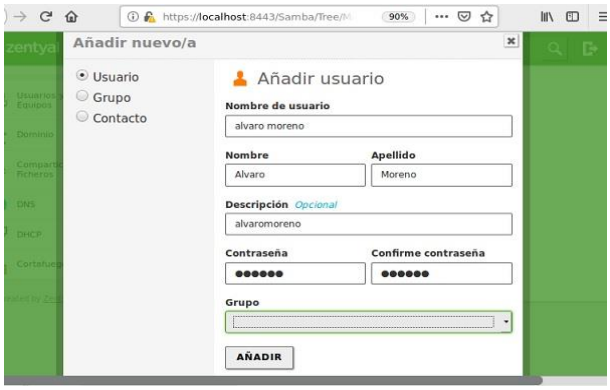


Imagen 20. Creación usuaria en el dominio.

Evidenciamos la creación del usuario:

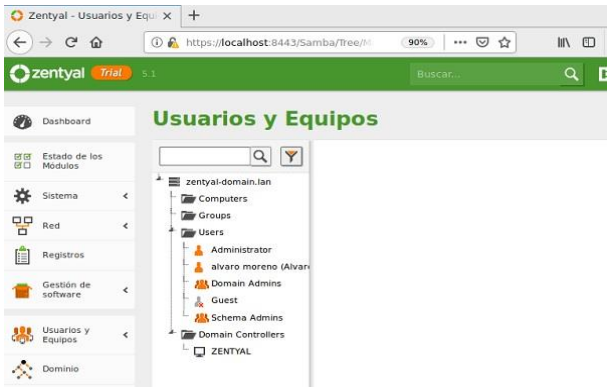


Imagen 21. Evidencia usuario creado en el dominio.

2. Proxy No Transparente:

Producto esperado: Implementación y configuración detallada del control del acceso de una estación GNU/Linux Ubuntu Desktop a los servicios de conectividad a Internet desde Zentyal a través de un proxy que filtra la salida por medio del puerto 3128.

El proxy en el sistema Zentyal es uno de los servicios esenciales que trae la plataforma. Que ofrece una de las opciones más seguras, para administrar y controlar la navegación de cada uno de los usuarios.

Las formas más comunes de configurar es darle una información del servidor proxy al navegador para que se efectué diferentes reglas, es decir que no cualquier usuario tenga acceso a internet, bloqueo de sitios web por medio de una lista negra que los usuarios no puedan ingresar, límite de consumo de ancho banda, archivos permitidos para ver y descargar, tiempos de permiso, todo ello hace que el proxy no transparente sea el más utilizado en las empresas.

Proxy transparente:

El proxy transparente no tiene la necesidad de especificar ninguna configuración del navegador ya que la propiedad del proxy esta de forma automática sin proxy, no hay que agregar la ruta de un servidor, ni un puerto proxy.

Se muestra la opción chuleada y se ven los cambios y configuración, sin necesidad de realizar configuración en los clientes.

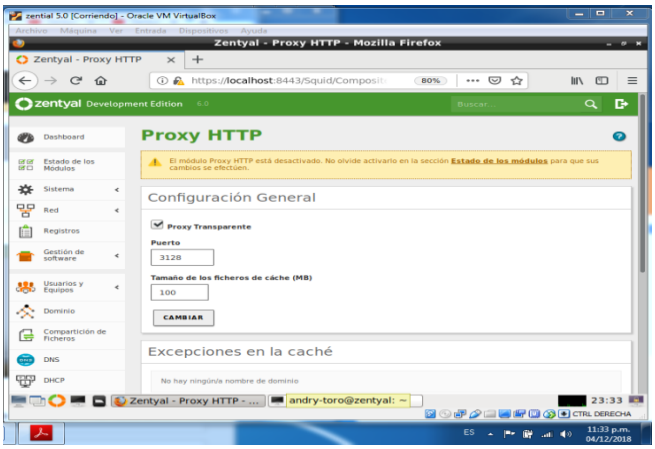


Imagen 22. Proxy transparente.

Proxy No transparente:

Debe de especificar en cada equipo en el navegador que debe ingresar la ruta del servidor, para tener seguridad, por ejemplo que no pueda ingresar a páginas no deseables, que no cualquier equipo pueda ingresar sin autorización, es decir sin las configuraciones no se puede acceder a internet, ya que el proxy es el que da el acceso, solo se puede ingresar de acuerdo a las directivas dadas.

Configurar el proxy HTTP no transparente, también se le llama proxy explicito, ya que este se le debe proporcionar información del proxy al navegador para que se conecte o aplique las directivas aquellas páginas web

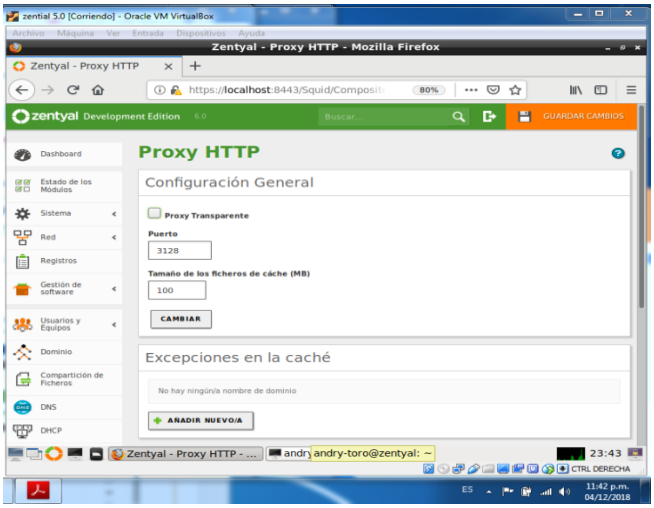


Imagen 23. Proxy no Transparente.

Habilitar módulos proxy HTTP y controlador dominio y NTP

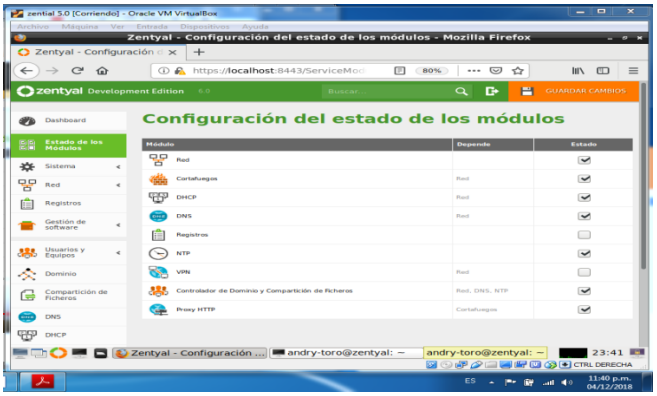


Imagen 24. Habilitar módulos.

Ir Configurar cortafuegos, para aumentar la seguridad de la red y el control de acceso de red, habilitar cortafuegos y denegar acceso HTTP y HTTPS.

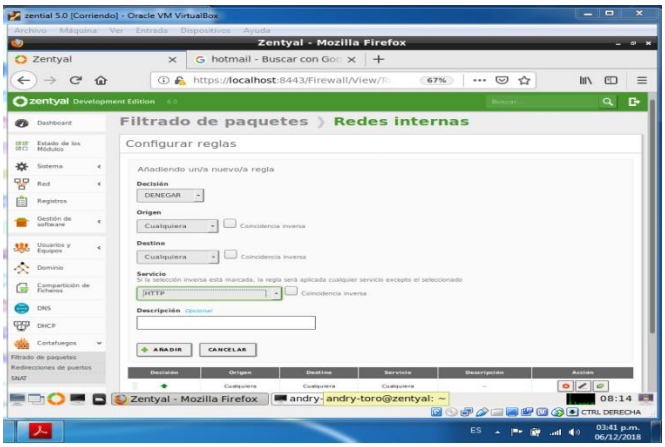


Imagen 25. Configurar cortafuegos.

Menú de configuración de reglas de filtrados paquetes cortafuego.

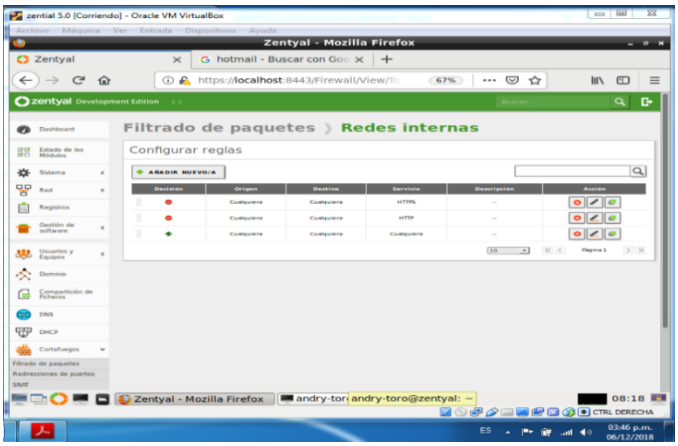


Imagen 26. Filtrados paquetes cortafuego.

Después de habilitar el proxy no transparente hay que ir a configurar el navegador para agregarle el proxy, hay que ir al navegador de un cliente y hacer la configuración del navegador e ingresarle el proxy correspondiente a la dirección IP del servidor Zentyal y el puerto 3128.

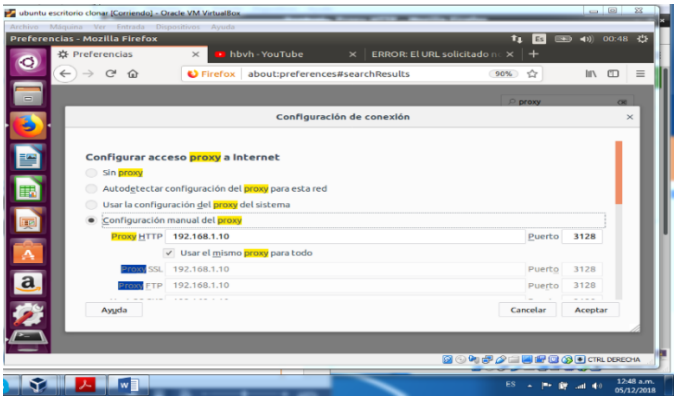


Imagen 27. Configuración proxy en el navegador Firefox.

Verificar si hay internet.

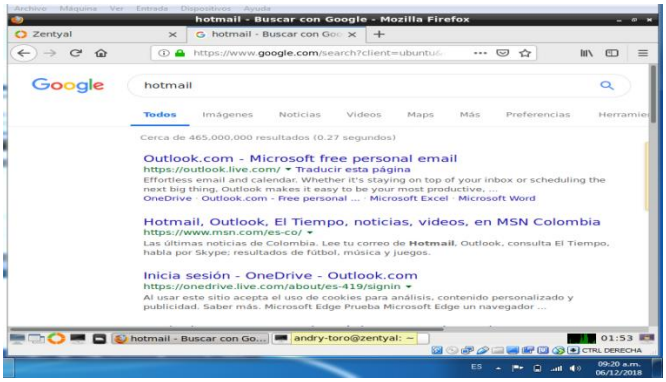


Imagen 28. Buscador de google.

Siguiente paso crear un perfil de filtrado, para luego hacer las configuraciones de bloquear, categorías dominios dependiendo de las extensiones de los sitios web, en tipos Mime permitir ejecutar archivos en las páginas dependiendo del tipo, ejemplo (audios (mpeg), animaciones o imágenes en flash (shockwave-adobe) y java, comprimidos Zip y gzip) etc.

Para crear bloqueos de páginas, hay que hacer los siguientes pasos Crear un perfil de filtrado por ejemplo general.

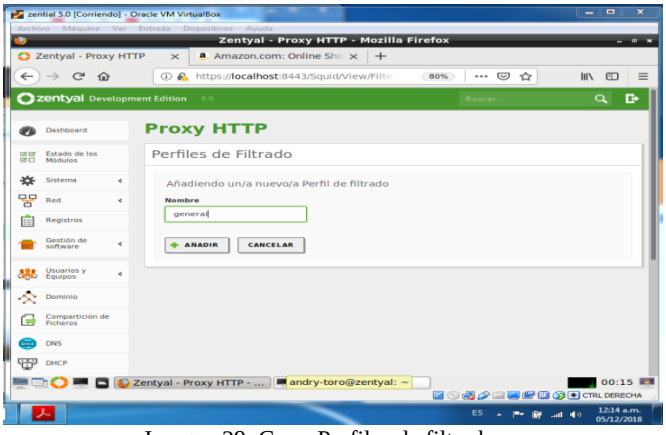


Imagen 29. Crear Perfiles de filtrado.

Se muestra el perfil creado con la opción de configurar.

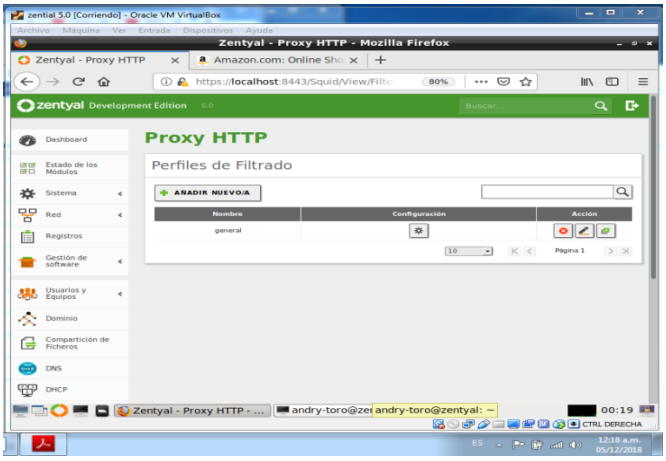


Imagen 30. Menú de perfiles de filtrado.

Ir a la configuración del perfil.
Es la opción umbral de filtrado y añades escoger la opción medio.

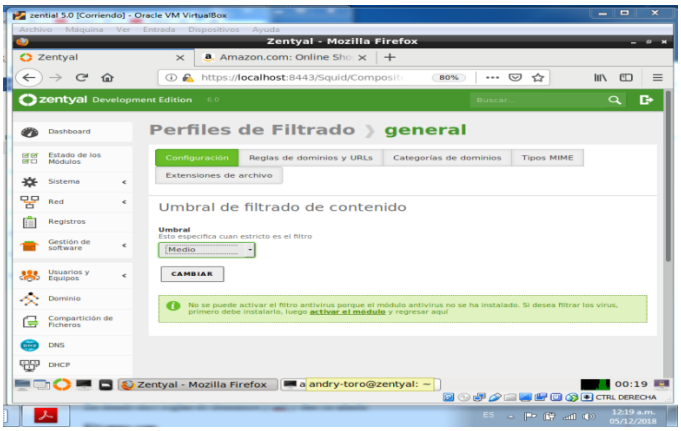


Imagen 31. Configuración de perfiles de filtrado, umbral.

Después ir a la opción de dominio y URLs
En la parte donde dice reglas de dominios y das en añadir

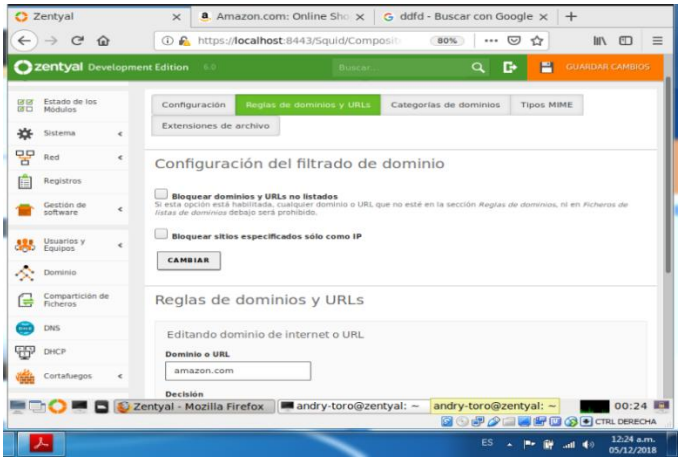


Imagen 32. Configuración proxy de perfiles de filtrado, dominio y Urls.

Se ingresa los dominios de las páginas a bloquear
Amazon.com
Eltiempo.com

Imagen 33. Configuración proxy, perfiles de filtrado, reglas de dominio.

En la opción categorías dominios
En la opción de mostrar extensiones

Se deja por defecto permitiendo todas las extensiones que puede tener archivos de un sitio web.

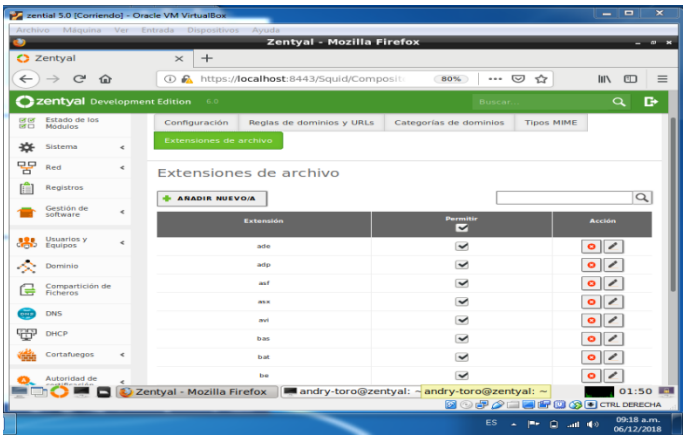


Imagen 34. Configuración proxy de perfiles de filtrado, categorías dominios, extensiones de archivo.

En la opción tipos Mime permitir ejecutar archivos en las páginas dependiendo del tipo, en este caso se deja como esta por defecto permitiendo todo.

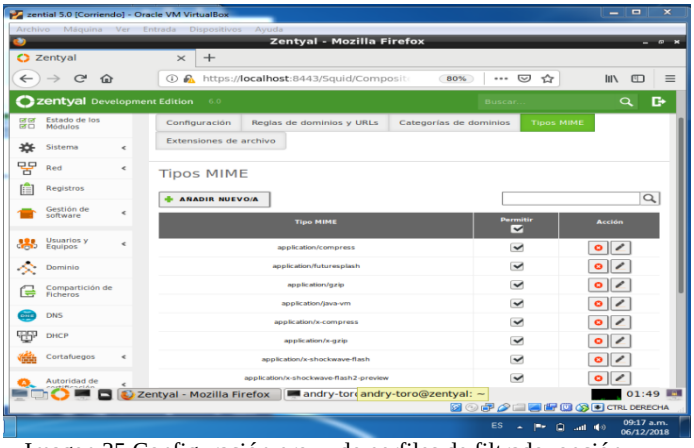


Imagen 35 Configuración proxy de perfiles de filtrado, opción tipo Mime.

Hay que ir a la opción de proxy reglas de acceso, le das en el botón editar, en esta opción puedo aplicar por periodos de tiempo que se

muestre esas reglas o por semanas o dependiendo reglas a seleccionar.

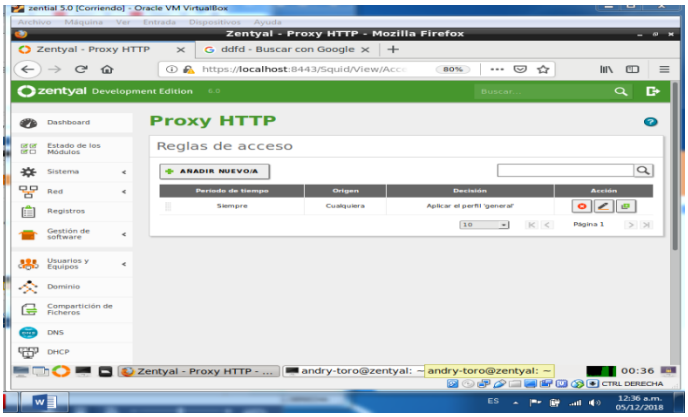


Imagen 36. Configuración proxy, reglas de acceso.

En la opción decisión, yo le doy en denegar todo o permitir a todo, dependiendo del perfil que se crea, se da en la opción aplicar dependiendo del perfil general que se creó anteriormente.

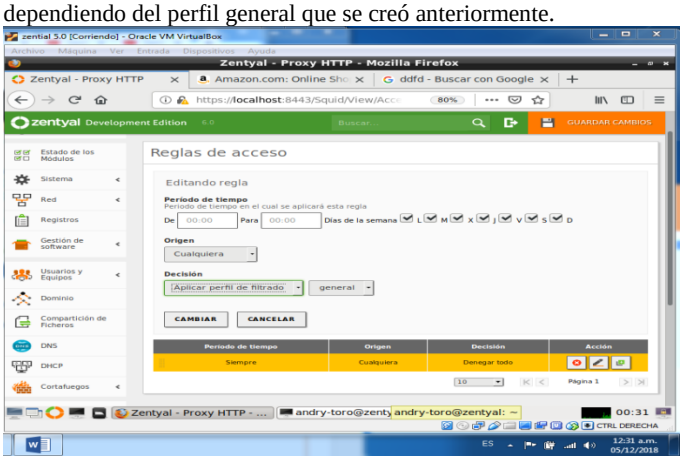


Imagen 37. Configuración proxy de reglas de acceso.

En la opción de proxy lista de categorías, opciones que tiene para añadir nuevas categorías.

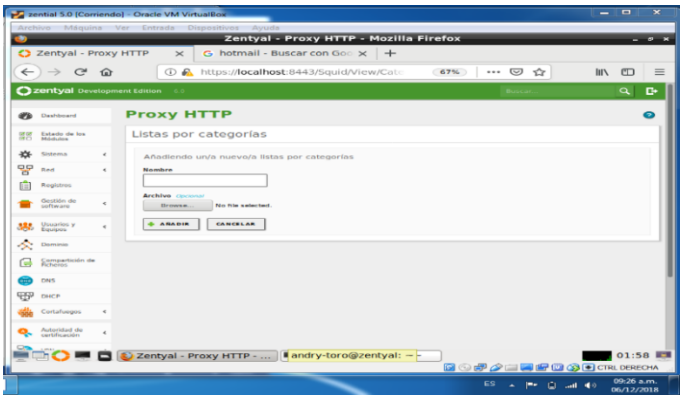


Imagen 38. Configuración de proxy, lista categorías.

En la opción de proxy limite ancho banda, opciones que se muestran para configurar el límite, que quiere que tenga cada usuario o todos, para minimizar consumo de internet para usuarios que no lo requieren.

Quedo habilitado por defecto, pero sin ninguna restricción.

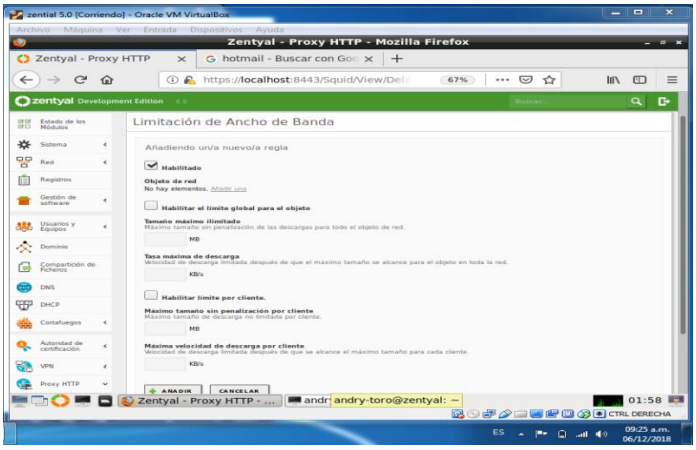


Imagen 39. Configuración de proxy, limitación ancho banda.

Después de configurar las opciones del proxy no transparente, y de configurar el perfil filtrado a las páginas que van a quedar en lista negra, las reglas de acceso por perfil o por todos, límites de ancho de banda a todos o por usuario.

Verificar si el cliente tiene habilitado la opción manual de proxy con los datos correspondientes explicados anteriormente

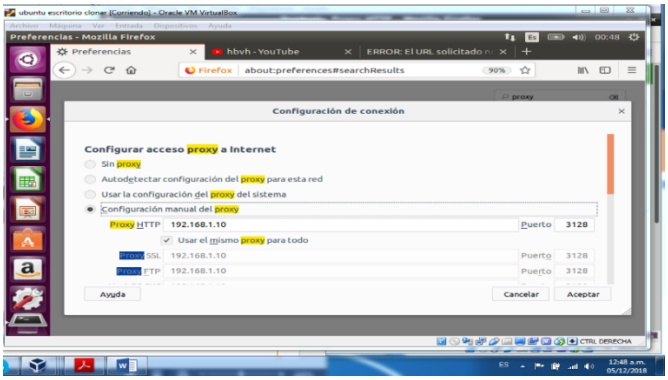


Imagen 40. Configuración navegador Firefox.

Se debe comprobar si las configuraciones dadas están funcionando en el cliente del sistema Ubuntu Desktop.

Se verifica si hay internet en otras páginas que no sea las bloqueadas como YouTube por ejemplo.

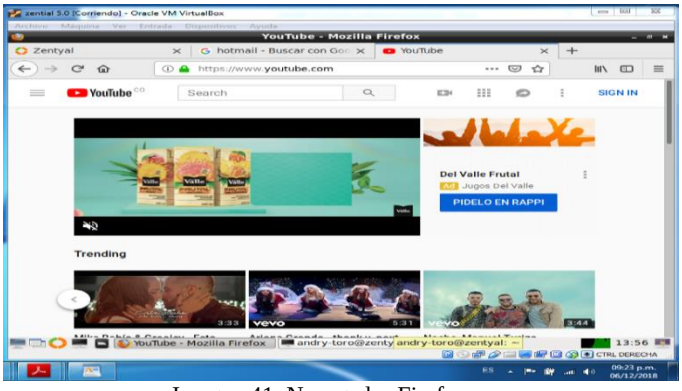


Imagen 41. Navegador Firefox.

Después se verifica las paginas bloqueadas y lo que se muestra, que el zentyal por medio del proxy no las deja seguir, solo se bloquean están direccionamiento HTTP, bloqueo página Amazon.com y eltiempo.com

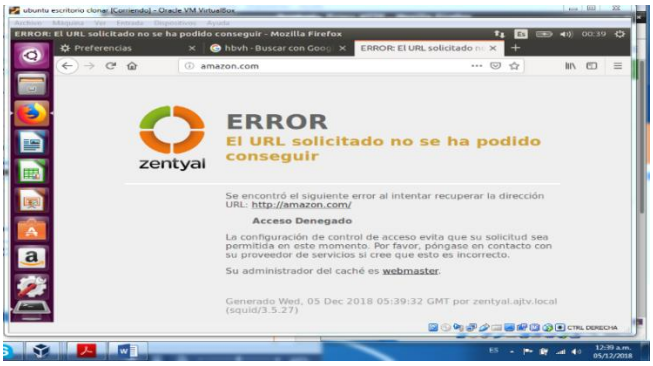


Imagen 42. Navegador, bloqueo páginas en lista negra

Al verificar las paginas bloqueadas que se configuro por medio del perfil de acceso, se pudo ver el funcionamiento de las directivas dadas al proxy HTTPS no transparente que se le dio al navegador del cliente, solo se ven estas directivas a los usuarios que estén dentro del rango de dirección IP dadas en el DHCP que tiene conexión con el servidor Zentyal.
También el proxy no deja navegar a internet a usuarios que no tiene configurado el servidor proxy.

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 Ubuntu Desktop.

Se instalan los paquetes de DNS Server y Firewall.

Imagen 43. Selección de paquetes a instalar.

Se da clic en continuar para que instalen los paquetes.

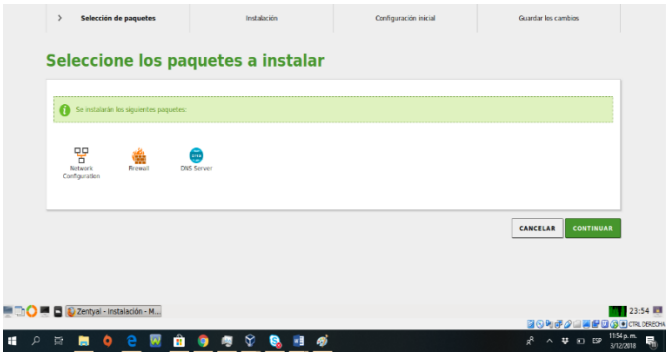


Imagen 44. Nombres de los paquetes a instalar.

Se configuran la interfaces de red eth01 es la externa y la eth1 (WAN) es la interna (LAN).

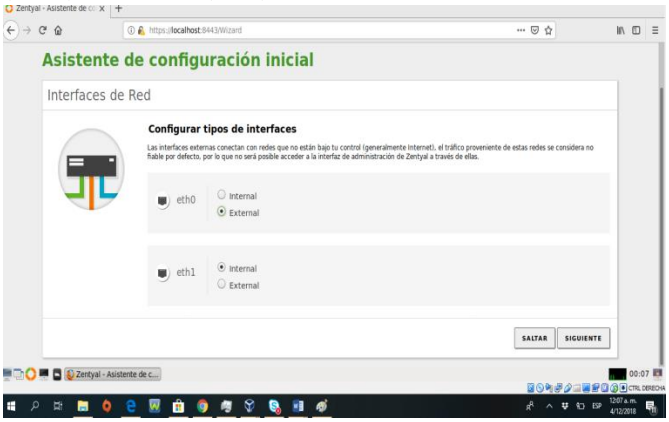


Imagen 45. Configuración tipos de interfaces.

Se configura eth0 como método DHCP y eth1 como método estático con la dirección IP 192.168.10.1

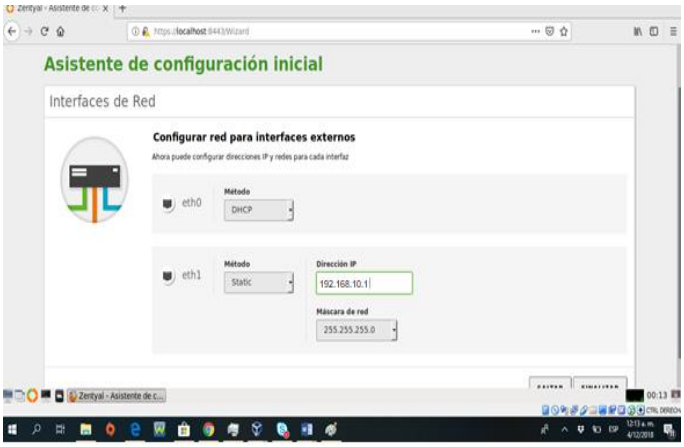


Imagen 46. Configuración red interfaces externos.

Se ingresa a Ubuntu y se configura la red manual para que se pueda conectar a través de la puerta de enlace a Zentyal Server.

Imagen 47. Configuración IP en Ubuntu desktop para conexión con Zentyal Server.

Se verifica las conexiones de red

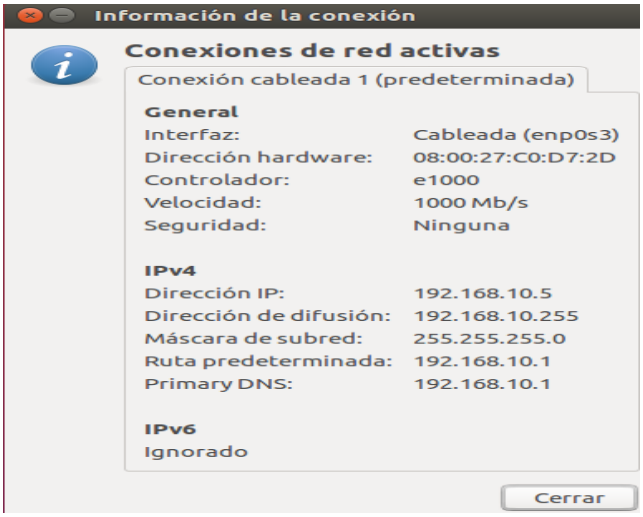


Imagen 48. Conexión de red activa.

Se ejecuta el comando ifconfig para mostrar las interfaces de red activas.

```
mayramoreno@mayramoreno-VirtualBox:~$ ifconfig
enp0s3    Link encap:Ethernet  direcciónHW 08:00:27:c0:d7:2d
          Direc. inet:192.168.10.5  Difus.:192.168.10.255  Másc:255.255.255.0
          ACTIVO DIFUSIÓN FUNCIONANDO MULTICAST  MTU:1500  Métrica:1
          Paquetes RX:46320 errores:0 perdidos:0 overruns:0 frame:0
          Paquetes TX:6178 errores:0 perdidos:0 overruns:0 carrier:0
          colisiones:0 long.colaTX:1000
          Bytes RX:11239173 (11.2 MB)  TX bytes:658682 (658.6 KB)

lo        Link encap:Bucle local
          Direc. inet:127.0.0.1  Másc:255.0.0.0
          Dirección inet6: ::1/128 Alcance:Anfitrión
          ACTIVO BUCLE FUNCIONANDO  MTU:65536  Métrica:1
          Paquetes RX:2545 errores:0 perdidos:0 overruns:0 frame:0
          Paquetes TX:2545 errores:0 perdidos:0 overruns:0 carrier:0
          colisiones:0 long.colaTX:1000
          Bytes RX:199676 (199.6 KB)  TX bytes:199676 (199.6 KB)
```

Imagen 49. Ejecución comando ifconfig.

Después vamos a Zentyal Server y en el cortafuegos se selecciona filtrado de paquetes y se selecciona Reglas de filtrado para las redes internas.

Imagen 50. Reglas de filtrado para redes internas.

Se da clic en añadir una nueva regla.

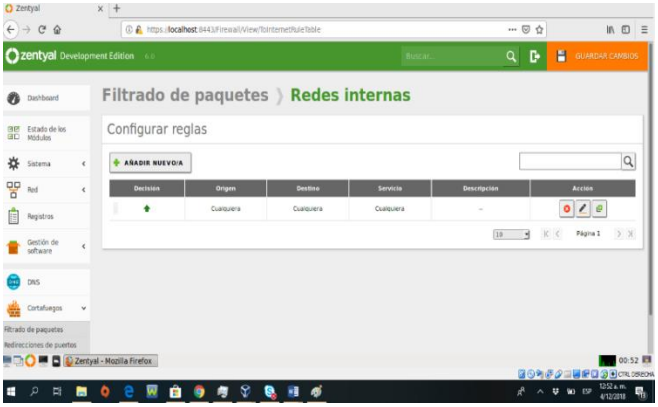


Imagen 51. Configuración reglas.

Se ingresa a la página www.youtube.com para evidenciar que se conecta a Internet.

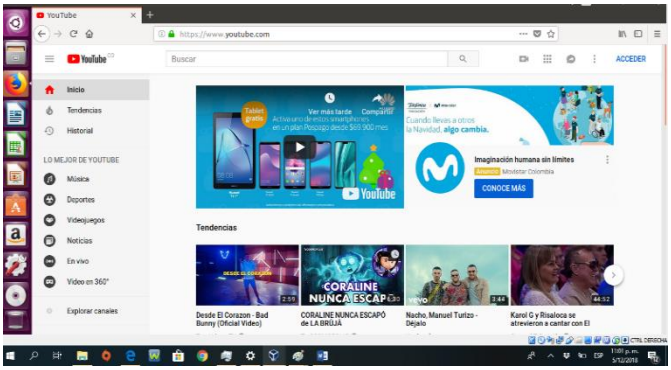


Imagen 52. Acceso a YouTube antes de aplicar la regla de filtrado.

Se añade la regla para denegar el acceso a YouTube. Se realiza ping para conocer la IP del sitio 172.217.28.110

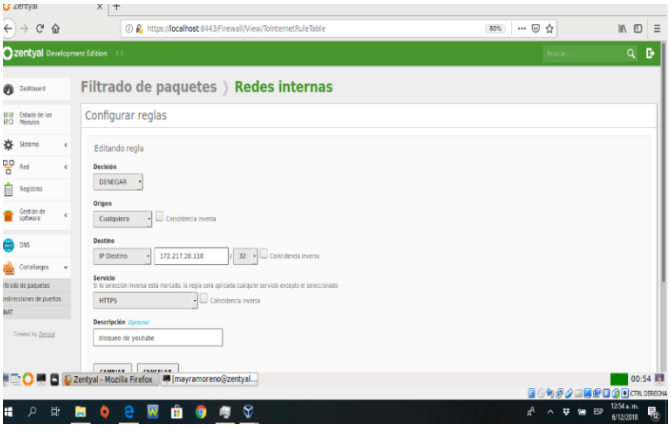


Imagen 53. Regla de filtrado para denegar ingreso a YouTube.

Se ingresa a la página de YouTube desde Ubuntu Desktop y no permite el acceso.

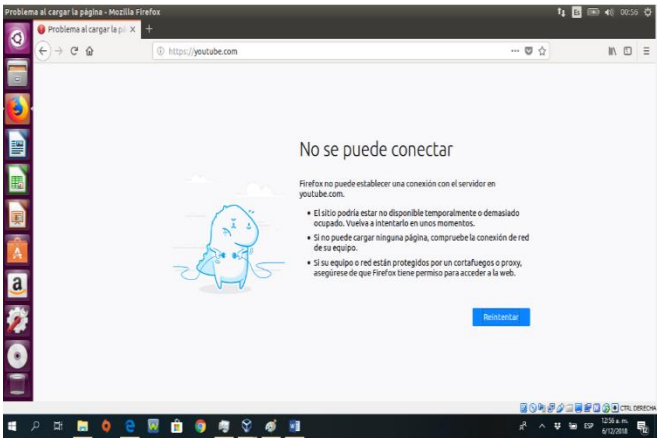


Imagen 54. Bloqueo a página de YouTube por el cortafuego.

Se ingresa a la página www.facebook.com para evidenciar que se conecta a Internet.

Imagen 55. Acceso a Facebook antes de aplicar la regla de filtrado.

Se ingresa a la página de Facebook desde Ubuntu Desktop y no permite el acceso.

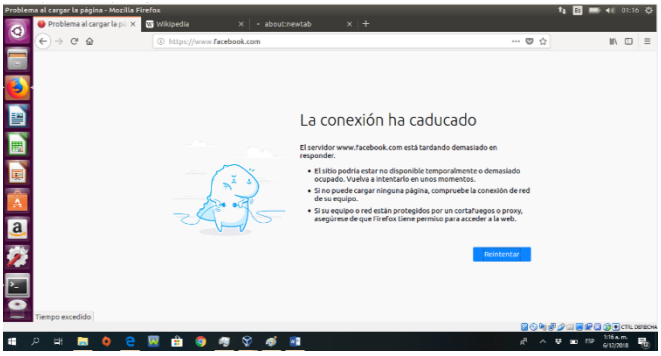


Imagen 56. Bloqueo a página de Facebook por el cortafuego.

Se ingresa a la página www.twitter.com para evidenciar que se conecta a Internet.

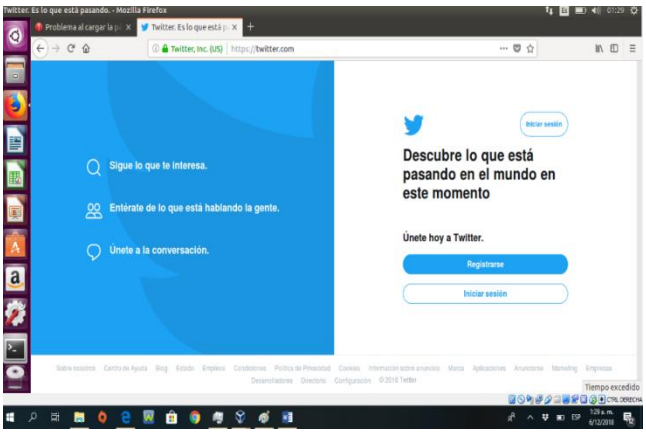


Imagen 57. Acceso a twitter antes de aplicar la regla de filtrado.

Se ingresa a la página de twitter desde Ubuntu Desktop y no permite el acceso.

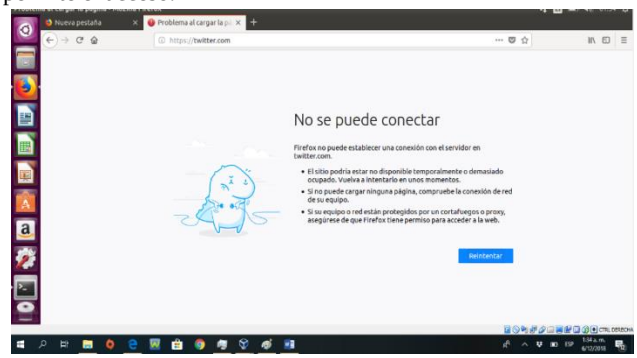


Imagen 58. Bloqueo a página de twitter por el cortafuego.

Se evidencia las reglas creadas para el bloqueo de los 3 sitios.

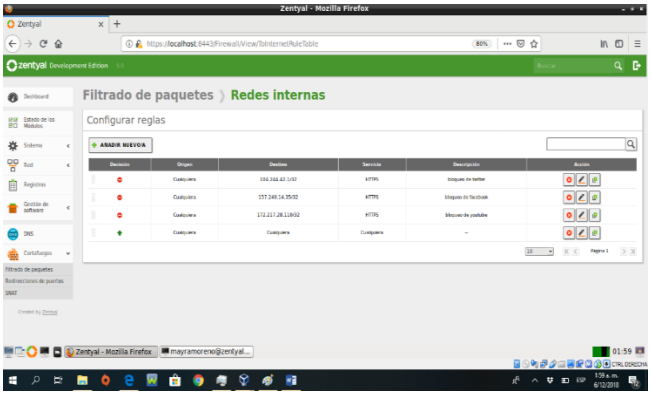


Imagen 59. Reglas aplicadas a 3 sitios web.

4. File Server y Print Server

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

Para la puesta en marcha del servicio de compartir archivos e impresoras se siguen los siguientes pasos:

Se instala el servicio Domain Controller and File Sharing, el cual seleccionamos una vez cargado Zentyal y damos Instalar.

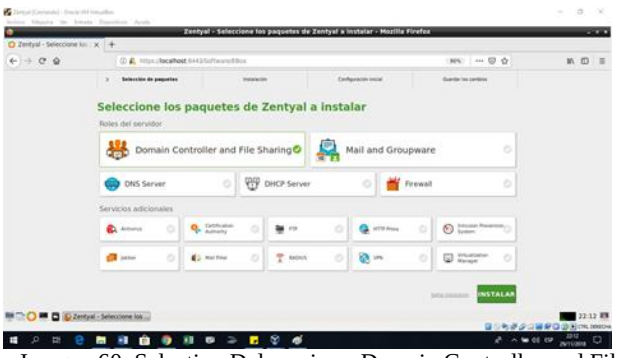


Imagen 60. Selection Del service a Domain Controller and File Sharing

Zentyal informa de las dependencias que serán necesarias para el módulo seleccionado anteriormente.

En el pantallazo siguiente damos clic en continuar.

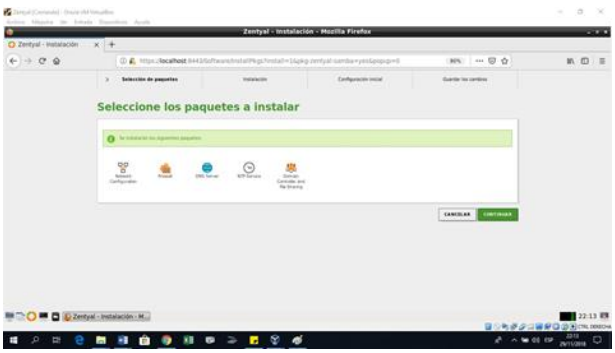


Imagen 61. Dependencias a Instalar.

Una vez terminado el proceso de instalación se solicitará información sobre la configuración de red, definiendo para cada interfaz de red si es interna o externa, es decir, si va a ser utilizada para conectarse a Internet u otras redes externas, o bien, si está conectada a la red local. Esta elección tendrá un impacto directo en las políticas del cortafuego, máscaras de red, interfaces en escucha por defecto para otros módulos, etc.

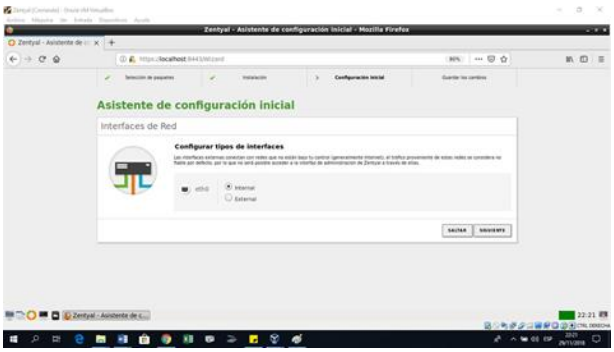


Imagen 62. Selección de Adaptadores de Red

Una vez configurada las interfaces creamos una cuenta de usuarios para poder ingresar. Para ello damos clic en la opción Usuario y Equipos -> Gestionar.

Luego daremos clic en la opción User y presionamos el botón +

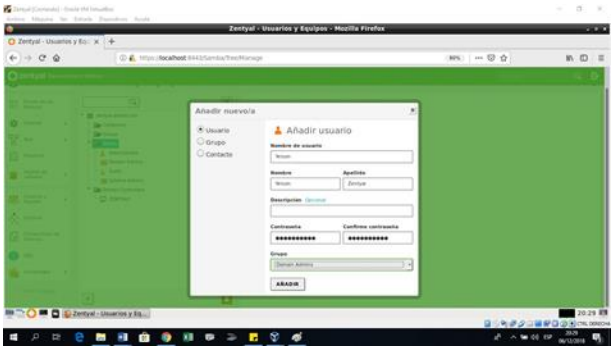


Imagen 63. Creación de Cuentas de usuario.

En el anterior pantallazo ingresamos los datos del usuario a crear y damos clic en Añadir

Para crear un nuevo directorio compartido, accederemos a Compartición de Ficheros -> Directorios compartidos y seleccionaremos Añadir nuevo

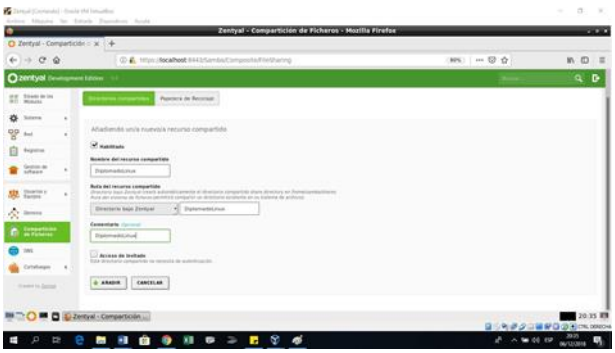


Imagen 64. Creación de Directorio.

Una vez creado se le dan los permisos necesarios a través de la opción de control de acceso.

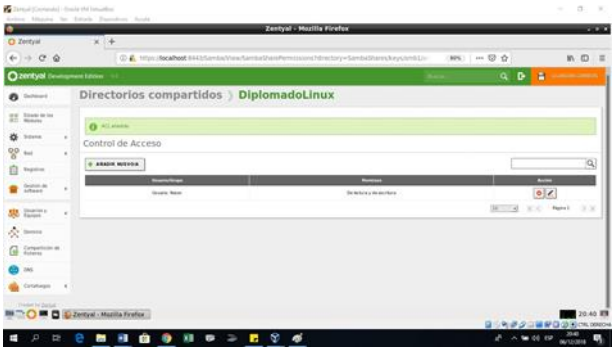


Imagen 65. Modificación de permisos.

Después de realizar todo el proceso anterior se debe unir la maquina cliente al dominio.

Unir equipo Ubuntu desktop a Dominio Zentyal

Abrimos la terminal de Ubuntu y nos dirigimos a la carpeta raíz del sistemas con el siguiente comando cd /etc y modificamos el archivo que establece nuestro servidor DNS, utilizando el siguiente comando sudo nano resolv.conf

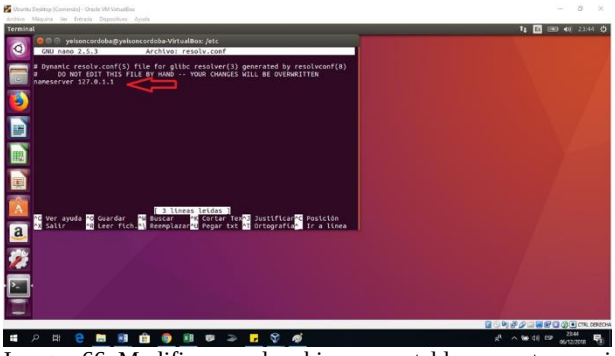


Imagen 66. Modificamos el archivo que establece nuestro servidor DNS.

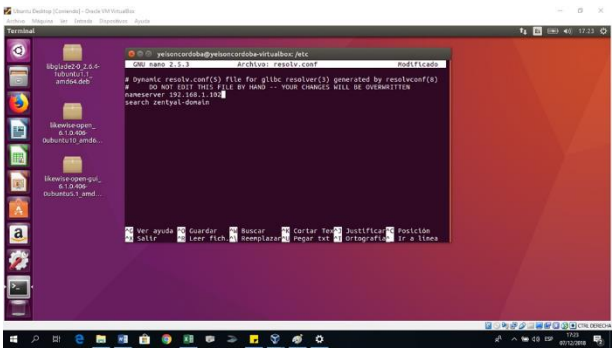


Imagen 67. Modificamos el archivo que establece nuestro servidor DNS.

Verificamos que haya conexión entre el Ubuntu desktop y el servidor Zentyal, para ello desde el desktop hacemos un ping a la dirección IP del servidor

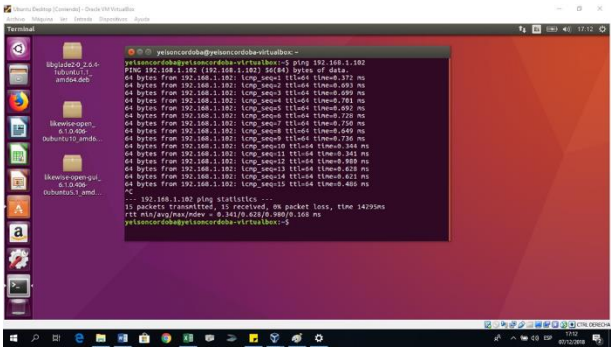


Imagen 68. Verificación de Conexión

Se instalan los siguientes archivos anteponiendo el comando sudo dpkg -i

- Libglade2-0_2.6.4-1ubuntu1.1_amd64.deb
- Likewise-open_6.1.0.406-0ubuntu10_amd64.deb
- Likewise-open-gui_6.1.0.406-0ubuntu5.1_amd64.deb

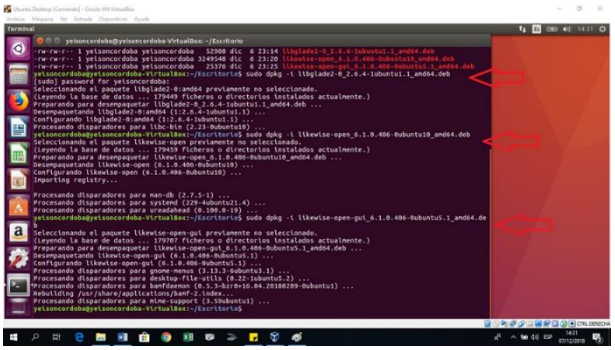


Imagen 69. Instalación para realizar la unión del Ubuntu desktop con Zentyal

Ejecutar el comando sudo domainjoin-gui para que se abra en modo gráfico y configuramos el nombre del equipo y el dominio

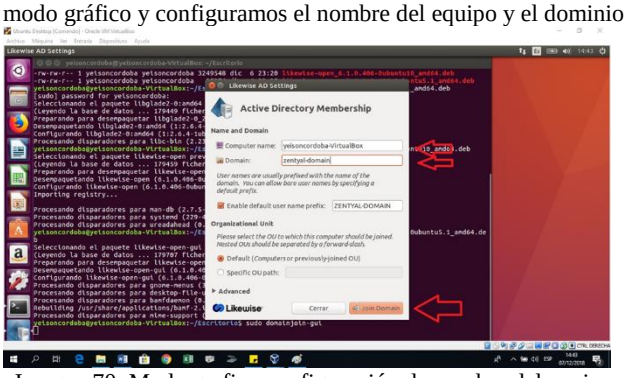


Imagen 70. Modo grafico configuración de nombre del equipo y dominio

Le doy clic en Join Domain nos solicitara el nombre de usuario y contraseña de Zentyal para realizar la conexión y reiniciamos la máquina para q se efectué la unión.

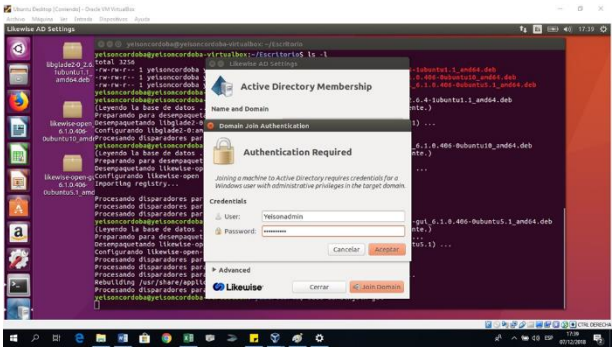


Imagen 71. Uniendo Cliente Windows a Dominio.

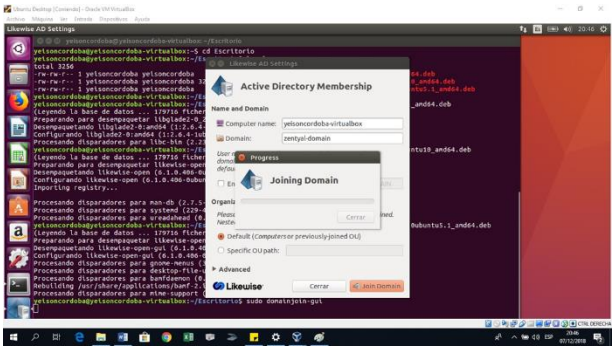


Imagen 72. Uniendo Cliente Windows a Dominio.

Agregando una Estación Windows 7 al dominio Zentyal.
Configuramos la tarjeta de red de Windows7, para ello nos vamos al centro de redes => cambiar configuración en el adaptador => damos clic derecho en el adaptador de red y nos vamos a propiedades => abrimos el protocolo de internet IPV4 => en servidor DNS preferido para poder unirnos escribimos la dirección IP de Zentyal y le damos clic en aceptar.

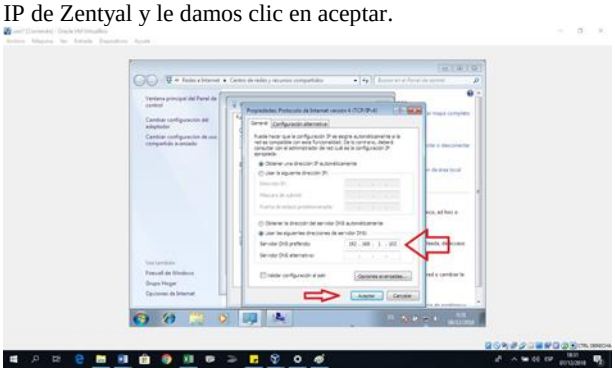


Imagen 73. Configurando Windows a Dominio

Ingresamos Propiedades del sistema, y configuramos el nombre del equipo y agregaremos el dominio (Zentyal-Domain).

Imagen 74. Uniendo Cliente Windows a Dominio.

Después de dar clic en aceptar, nos envía un pantallazo donde escribiremos las credencias de usuario y contraseñas de dominio creadas en Zentyal para poder llevar a cabo la unión

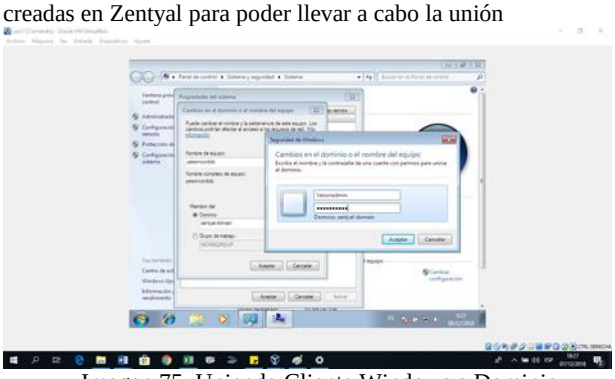


Imagen 75. Uniendo Cliente Windows a Dominio.

Ingresamos Propiedades del sistema, y configuramos el nombre del equipo y agregaremos el dominio.

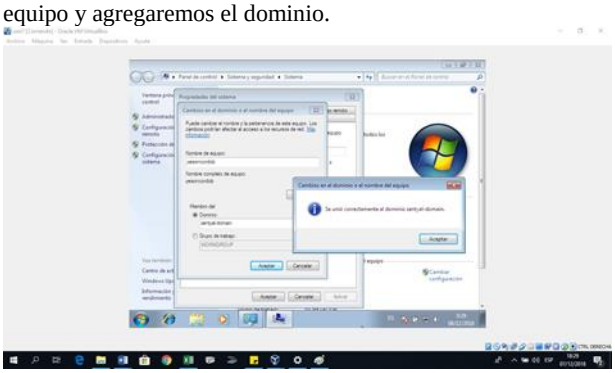


Imagen 76. Uniendo Cliente Windows a Dominio.

Una vez se reinicia Windows podemos ingresar bajo el dominio con nuestras credenciales creadas en Zentyal.

Imagen 77. Login Dominio.

Se crea una unidad de red personalizada donde podemos compartir información.

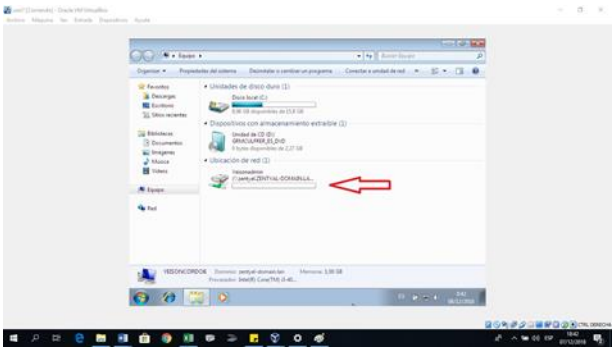


Imagen 78. Creación de unidad de red recurso compartido Dominio Zentyal.

Nos vamos a la red y digitamos la dirección de nuestro Servidor Zentyal y podemos observar las carpetas compartidas.

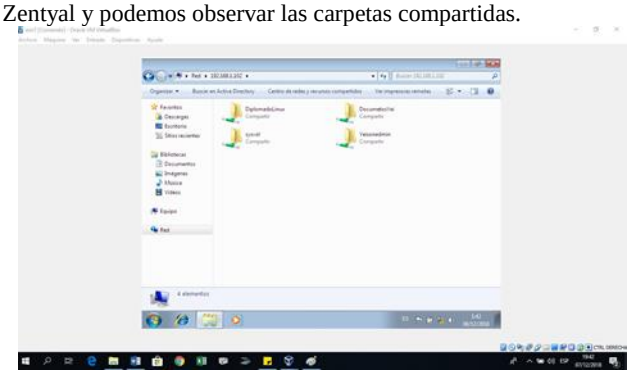


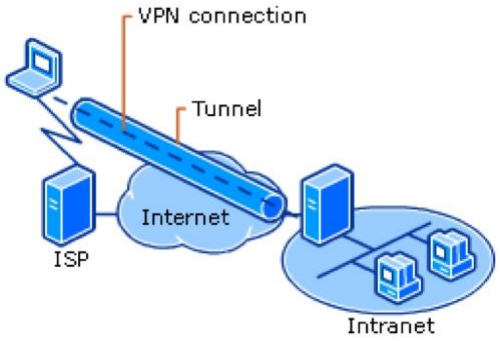
Imagen 79. Ingreso a recurso compartido Dominio Zentyal.

5. VPN

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 Ubuntu Desktop. Se debe evidenciar el ingreso a algún contenido o aplicación de la estación de trabajo.

VPN

Virtual Private Network (Red privada virtual), es una tecnología que nos permite crear una extensión segura de la LAN, a través de una red pública o no controlada como la WAN (Internet), esta tecnología ha sido utilizada ampliamente por las empresas para permitir a sus empleados conectarse desde distintos sitios geográficos a su intranet a través de internet, como si estuvieran físicamente en el mismo lugar, para obtener acceso a los recursos, información y aplicaciones de la compañía de forma segura, ya que una VPN no solo crea el camino por donde transitan los datos, sino que además los encripta.



Tomado de: http://www.chicageek.com/que-es-vpn-para-que-sirve/

Imagen 80. Diagrama funcionamiento VPN.

Normalmente un usuario por medio de sus dispositivos se comunica al modem del ISP, el cual trasfiere los datos y comunicaciones a internet, y por lo general este tipo de comunicaciones viajan en texto plano a través de la WAN, lo que significa que todos los puntos o rutas por donde paso la información podrían tener acceso a la misma, con una VPN el proceso de comunicación se hace desde tus dispositivos al modem, del modem al ISP y del ISP se va directo a tu VPN, y de ahí a internet y toda la información regresa de la misma forma con la ventaja que desde que sale desde tu dispositivo la comunicación va cifrada y encriptada lo que garantiza que ningún punto en el camino sabría el contenido.

Dentro de los usos principales de la VPN esta:

- El teletrabajo, conexión directa a la LAN desde cualquier sitio.
- Evitar la censura sobre contenidos, ya sea por parte de los ISP, proveedores de contenido, por política, geográficos, etc.
- Capa de seguridad extra en la comunicación.
- Red falsa para video juegos
- Anonimato y privacidad en la red, esta última es la más importante hoy por hoy.

Implementación Servidor VPN Zentyal:

Seleccionamos los paquetes de Zentyal a instalar, en este caso VPN, automáticamente Zentyal nos confirma los paquetes que serán instalados para la correcta puesta en marcha del servicio y la seguridad del sistema, instala la configuración de red, el cortafuego, autoridad de certificación y el módulo de VPN:

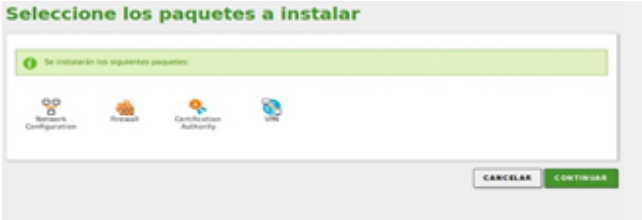


Imagen 81. Paquetes necesarios VPN Zentyal.

El sistema comienza con el proceso de instalación de módulos, en la interfaz de configuración de red la podemos definir como externa o interna, para el caso la vamos a definir como externa, lo que indica que desde cualquier red incluido internet con las debidas

credenciales, procesos de autenticación y configuración del modem de parte de nuestro ISP (puertos abiertos, DMZ, IP de redirección), se podría acceder por la VPN al servidor, la dejamos de tipo dinámica y esto es habitual donde se conectan múltiples maquinas al servidor Zentyal:

Imagen 82. Configuración tarjeta de red Zentyal

Pero recordemos que definir un sistema DHCP no ayuda a la seguridad del servidor, un administrador de red, antes de realizar la instalación tiene definido la RED, maquinas, IPs, que va a utilizar, incluso es posible para aumentar la seguridad, atar la IP con la MAC de la máquina, esto garantiza que cualquier acceso de tipo VPN de una IP no establecida y una MAC no concordante, no podrán acceder al servidor, al finalizar la instalación del servicio VPN, vemos la Dashboard Zentyal Server 5.1, edición comercial:

Imagen 83. Dashboard Zentyal en ejecución

Para poder crear una VPN en Zentyal Server debemos ingresar al panel de control, digitar el usuario y contraseña y dirigirnos al módulo de VPN, servidores, una vez el dashboard nos dirige nos encontramos con un mensaje que nos indica que se debe crear un certificado CA valido para usar los servidores VPN y nos presenta un enlace al módulo de autoridad de certificados, donde crearemos uno.
Al dar clic nos dirige a una página donde iniciamos la autoridad de certificados, creando el primer certificado con el cual validaremos los demás certificados, colocamos el nombre de la organización, el código del país, la ciudad y el estado son opcionales por lo tanto no los vamos a editar, un cuarto campo nos valida los días de validez de nuestro certificado, para la práctica vamos a usar un total de 100 días:

Imagen 84. Creación de certificado en Zentyal.

Ahora ya volvemos al módulo de VPN, servidores y ya nos muestra el panel de control donde crearemos el servidor VPN, damos clic en añadir nuevo, colocamos el nombre del servidor y damos en guardar cambios, nos muestra el servidor habilitado y damos clic en configuración, para ver los parámetros por defecto, los cuales pueden ser cambiados:

Imagen 85. Creación de servidor VPN en Zentyal.

En configuración, tenemos el puerto, rango de IPs del servidor, nombre del certificado y habilitamos la interfaz TUN (Modo de funcionamiento capa 3), definimos todas las interfaces y damos clic en guardar cambios:

Imagen 86. Configuración servidor VPN Zentyal.

Vamos a VPN, servidores y damos clic en descargar paquete de configuración de clientes, Zentyal nos informa que no hay ningún certificado creado para los clientes, se debe crear un certificado por cada cliente conectado que tengamos, al dar clic nos dirige a la autoridad de certificados de clientes para crear los necesarios.

Vamos a crear dos certificados uno con el nombre de cliente_leonardo y otro con el nombre de cliente_celeita, por defecto nos aparece el número de días máximo del servidor damos en expedir:

Imagen 87. Creación certificados clientes VPN Zentyal.

Volvemos a VPN, servidor y descargar paquete configuración del servidor del cliente:

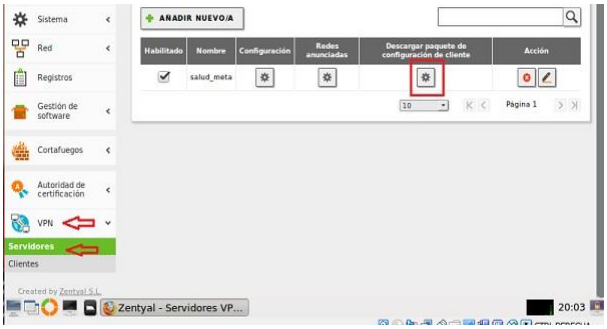


Imagen 88. Descarga de paquetes clientes servidor VPN Zentyal.

Nos presenta una pantalla donde definimos el tipo de cliente, Linux, el nombre del cliente, seleccionamos cliente_leonardo y la dirección del servidor, lo que viene al caso la IP publica de nuestra red, siempre y cuando hubiéramos contactado a nuestro ISP para que en el modem nos abriera el puerto, nos creara una zona DMZ y redirigiera el tráfico a la IP interna del servidor Zentyal, por ahora en una terminal haremos un ifconfig y tomaremos la dirección que nos asigna la tarjeta de red:

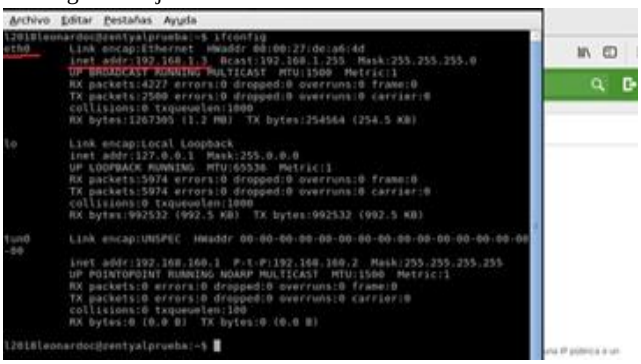


Imagen 89. Ifconfig terminal Zentyal.

Colocamos los datos y damos clic en descargar y guardamos el archivo, terminado este proceso cerramos la interfaz gráfica o el panel de control del servidor Zentyal, nos dirigimos al home descargas y le pasamos el archivo descargado al cliente, ya sea por correo electrónico, medio magnético, etc.

Imagen 90. Configuración paquete para cliente.

Llegado a este punto tenemos que decir que para el funcionamiento o puesta en marcha del VPN en el cliente, Zentyal echa mano de una herramienta de conectividad basada en software libre y protocolos SSL (Secure Sockets Layer) que es OpenVPN, la cual ofrece conectividad punto a punto con validación jerárquica de usuarios y host conectados remotamente, esta publicada bajo licencia GPL de software libre, (*tomado de: https://es.wikipedia.org/wiki/OpenVPN*).

Abrimos nuestra maquina Ubuntu desktop e instalamos OpenVPN con el comando **sudo apt-get install openvpn**:

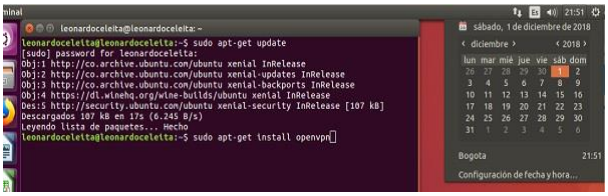


Imagen 91. Instalación OpenVPN, Ubuntu Desktop

Una vez instalado OpenVPN se debe editar el archivo openvpn ubicado en la ruta /etc/default/openvpn y desconectar el estado AUTOSTART=”none” para que el VPN no se conecte siempre, con el archivo descargado del servidor Zentyal, se traslada a Ubuntu-desktop se descomprime y copia los 4 archivos en la siguiente ruta, /etc/openvpn/, mediante el siguiente comando **sudo cp *.* /etc/openvpn/**, esto ubicado en la carpeta Descargas de nuestro home.

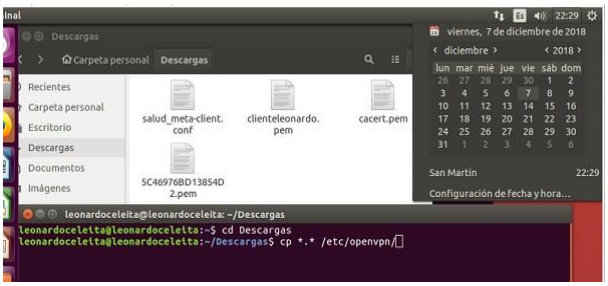


Imagen 92. Archivos de cliente en maquina Ubuntu.

Aquí hacemos una copia del archivo *.conf a solo client.conf con el comando, **sudo cp salud_meta-client.conf client.conf,** ahora se debe editar el archivo client.conf, en las líneas que dice ca, cert, key, le quitamos las comillas dobles a las tres líneas, quedando de la siguiente manera.

Imagen 93. Configuración archivo client.conf VPN.

Prueba de conexión

En este punto vamos a realizar un ifconfig en la maquina Ubuntu-desktop para verificar que interfaces de red tenemos activas y la IP 192.168.1.5:

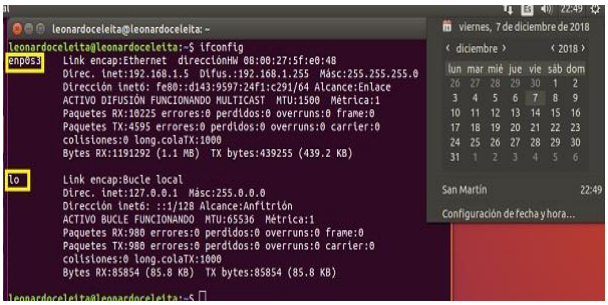


Imagen 94. Ifconfig cliente Ubuntu desktop.

Como se observa en la imagen solo nos lista dos puntos de acceso la tarjeta de red y el localhost, tratamos de conectarnos a la interfaz de administración del Zentyal en el Ubuntu desktop, digitando en el navegador https://192.168.160.1:8443/login/index y obtenemos el siguiente resultado

Imagen 95. No comunicación entre el servidor y el cliente.

Demostrando que no hay conexión, para activar nuestra VPN debemos estar ubicados en la siguiente dirección /etc/openvpn/ y digitar el siguiente comando, **sudo openvpn /etc/openvpn/client.conf**, al dar enter y digitar la contraseña, empieza a realizar el proceso de conexión con la maquina Zentyal, debemos esperar a que nos muestre el mensaje sequence completed, podemos ver que el servidor Zentyal nos otorga una IP del rango de direcciones que le habíamos predefinido:

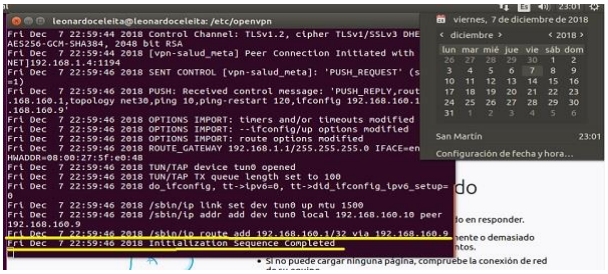


Imagen 96. Ejecución de la VPN en el cliente.

Hacemos un ifconfig para verificar las rutas de conexión que tenemos.

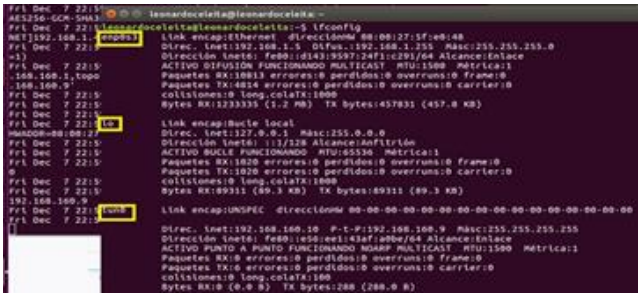


Imagen 97, Ifconfig Ubuntu, VPN túnel creado.

Podemos observar que nos creó una tercera conexión de tipo tun0 o tipo túnel, a este punto ya podemos decir que existe una conexión tipo VPN entre el Ubuntu-desktop y el servidor Zentyal, desde el mismo rango IP del servidor o red LAN, para verificar le damos recargar al navegador Firefox y vemos ejecutando el administrador del Zentyal en el Ubuntu.

Imagen 98. Comunicación VPN Ubuntu y servidor Zentyal.

IV. CONCLUSIONES

Con la implementación de la distribución Zentyal y los diferentes servicios podemos concluir que la herramienta que proporciona la plataforma Zentyal es muy fácil de manejar, dando solución en la gestión a la red. Cada uno de los módulos hacen unas tareas para proporcionar que la red se maneje de manera interna o externa y se puedan conectar diferentes usuarios por medio del servidor, configurando los métodos para asignar las directivas correspondientes para que obtenga conexión, acceda a internet y

obtenga seguridad llevando a cabo cada uno de los procesos que sumista cada uno de los servicios.

El proxy no transparente es uno de los servicios más utilizado en las empresas por su seguridad y restricciones que proporciona, ya que cuenta con unas directivas de acceso, es decir si algún usuario no cuenta con esas directivas no puede ingresar a navegar en internet, para su funcionalidad el navegador de cada cliente debe proporcionarle la ruta del servidor y puerto para su puesta en marcha. Además, esas directivas al configurarse, las acciones que toma es no dejar entrar a páginas no deseadas, de acuerdo al perfil del usuario, de acuerdo a la extensión del archivo y dependiendo de las categorías que maneja el sitio web, y muchas más limitaciones que hace que garantice mejor navegación.

Finalmente al aplicar las reglas de filtrado para redes internas en el cortafuegos de Zentyal, se evidencio el bloqueo de 3 páginas en el escritorio de Ubuntu. También es muy importante tener en cuenta que se debe hacer ping en las páginas para conocer las IP y así poder aplicar las reglas de filtrado.

Una VPN no solo garantiza confidencialidad y seguridad de la información que manejamos y trasmitimos a través de las redes para la empresas, si no que agrega una capa extra en la protección contra el ciber-crimen y nos brinda privacidad para que nuestros datos personales, costumbres y gustos en internet no se conviertan en mercancía para los monopolios que rastrean, monitorizan y almacenan datos en internet, por si no lo has notado cada vez la publicidad que ves en un sitio de internet va dirigida de acuerdo a tus búsquedas o costumbres en internet.

V. REFERENCIAS

[1] zambrano, r. (s.f.). *01. Curso Práctico de Zentyal - Instalación de Zentyal listo y preparado para Instalar* . Obtenido de https://www.youtube.com/watch?v=hW-oLbCNj5I

[2] JGAITPRO. (s.f.). *Zentyal - Configurar Proxy Web HTTP No Transparente.* Obtenido de https://www.youtube.com/watch?v=PG7pcYmBkw4&t=249s

[3] JGAITPRO. (s.f.). *Zentyal - Instalar y configurar Proxy Web HTTP Trasparente.* Obtenido de https://www.youtube.com/watch?v=X54YKfeFQhQ

[4] JGAITPTO. (s.f.). *Zentyal - Bloquear sitios web por HTTP*. Obtenido de https://www.youtube.com/watch?v=73z1T_NIGZI

[5] Red Orbita (07-11-2016) Instalación y configuración de Zentyal Server 5. Obtenido de: http://red-orbita.com/?p=7634

[6] Andrés Mora (04-04-2017) Instalación Zentyal 5.0. Obtenido de: https://www.youtube.com/watch?v=5N9upYznnCo

[7] Ramírez D. (09-12-2013) Controlador de Dominio (LDAP) Zentyal. Recuperado de: https://www.youtube.com/watch?v=mPMbAphTiXw&t=2405s

[8] Goujon, A., & Goujon, A. (2012). *¿Qué es y cómo funciona una VPN para la privacidad de la información?*. *WeLiveSecurity*. Retrieved 1 December 2018, from https://www.welivesecurity.com/la-es/2012/09/10/vpn-funcionamiento-privacidad-informacion/

[9] *En/5.0/Virtual private network (VPN) service with OpenVPN - Zentyal Linux Small Business Server*. (2018). *Wiki.zentyal.org*. Retrieved 8 December 2018, from https://wiki.zentyal.org/wiki/En/5.0/Virtual_private_network (VPN)_service_with_OpenVPN