

Instalación y configuración de un server zentyal 6.0 y un cliente Ubuntu, accediendo a los servicios de DHCP, Proxy no transparente, Cortafuegos, File server y VPN

Manuel Ramírez Galvis, Herney Galvis Rivera, Víctor Urrego Bejarano, John Alexander Baquero,
Escuela de ingeniería, Universidad Nacional Abierta y a Distancia UNAD
Bogotá, Colombia

profe.fernandorg@gmail.com
herneygalvis@gmail.com
victorurrego@hotmail.com
jhonalexanderb@gmail.com
devia.j@hotmail.com

Resumen: A continuación, se realizarán diferentes instalaciones, actualizaciones e implementación y puesta en marcha de aplicaciones y contenidos Web. El servidor se implementará mediante una máquina virtual en el cual se instalará y configurará todo lo necesario para ofrecer la alta disponibilidad. Para finalizar el trabajo se realizará una verificación del funcionamiento del servidor configurado. El trabajo se centra en la instalación, configuración y evaluación de un servidor web de alta disponibilidad.

Abstract-- Then, different installations, updates and implementation and implementation of Web content and applications will be carried out. The server will be implemented through a virtual machine in which everything necessary to offer high availability will be installed and configured. To complete the work, a verification of the operation of the configured server will be carried out. The work focuses on the installation, configuration and evaluation of a high availability web server.

Palabras Clave: Servidor, Cliente, Zentyal, Dominio, Proxy, Cortafuegos, VPN, Usuario, Interfaces, IP.

I. INTRODUCCIÓN

Utilizando los aprendidos en el diplomado en Software libre Linux basado en su versión 16.04 desktop, usando el Software de servicios Zentyal 6, así como el VirtualBox en su versión 5.52 se instalarán máquinas virtuales en las cuales se implementará la solución a 5 temáticas establecidas, se instalará un servidor Zentyal y un cliente Linux Ubuntu, el cual accederá a los servicios de datos y red para poder funcionar dentro de ámbitos laborales y académicos. Las modificaciones del servidor que presta los servicios serán realizadas en el Dashboard original del Zentyal 6, una interfaz web bastante amigable y fácil de utilizar, cuyas modificaciones se verán reflejadas en el uso de los servicios del cliente Ubuntu 16.04 enfocados en las temáticas de seguridad y propiedades de la red.

Tabla 1 Roles y temáticas grupo 201494_6		
Nombre	Roll	Temática
Herney Galvis Rivera	Alertas	

		DHCP Server, DNS Server y Controlador de Dominio
Manuel Fernando Ramirez Galvis	Entregas	Proxy no transparente
Victor urrego		Cortafuegos
Jorge debia		File Server y Print Server
John Alexander Baquero	Revisor	VPN

II. INSTALACIÓN DE ZENTYAL SERVER 6.0

2.1 Requisitos de Instalación

Zentyal es un software muy liviano que requiere: Procesador de 2GHz (duocore, celeron M), 3 Gb RAM (DDR2 o DDR3), Disco duro de 250 Gb, Tarjeta de red 10/100.

La instalación en una máquina virtual requiere de un sistema operativo base de 64 Bits y para poder realizar la instalación en Virtual box en sus versiones 4.4 en adelante con el complemento de requerimientos para reconocimiento de USB compatible para todas las versiones.

El Servidor Zentyal incorpora todos los servicios de red necesarios en pequeñas y medianas empresas y lo que es más importante, ofrece la primera implementación nativa de Microsoft Active Directory® en Linux que es fácil de usar

Características técnicas:

- Basada en Ubuntu Server 16.04.3 LTS
- ISO híbrido con soporte a BIOS y UEFI
- Integración de la última versión estable de Samba (4.6.7)
- Integración de la última versión de SOGo (3.2.10)

- Resolución de problemas de instalación en Hyper-V y otras plataformas de virtualización o hardware específico

2.2 Link de descarga

La versión 6.2 de Zentyal ya está disponible, para ser descargada por medio de la inscripción en la cual el usuario llenara un formulario y con este la empresa hará llegar un correo con la clave para poder tener la versión de prueba de 45 días (TRIAL), en un formato ISO
<http://www.zentyal.com/es/zentyal-server/trial/>

2.3 Instalación

Creamos la nueva máquina virtual de 64 bits Ubuntu asignándole un nombre y configuramos el adaptador de red para que tome los datos desde un adaptador puente de la Wifi o de la red que tengamos en el quipo, en Zentyal se deben dejar dos adaptadores de red, no solo uno y los dos deben estar configurados como puente

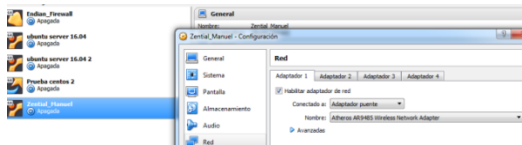


Imagen 1. Selección de adaptador de Red

Iniciamos la maquina seleccionamos el disco y seleccionamos el idioma

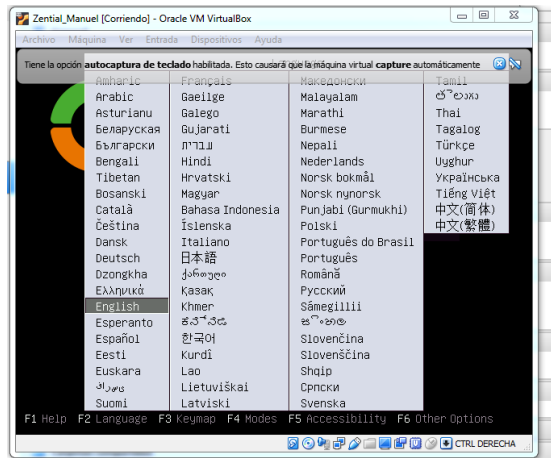


Imagen 2. Selección de Idioma

Seleccionamos instalar



Imagen 3. Selección del tipo de instalación

Seleccionamos territorio de nuestra ubicación

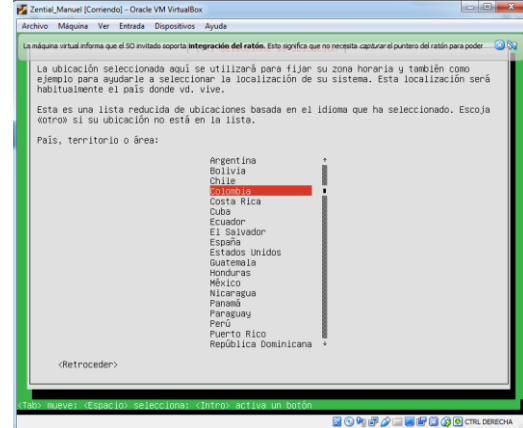


Imagen 4. Selección de País de ubicación

Escogemos distribución de teclado

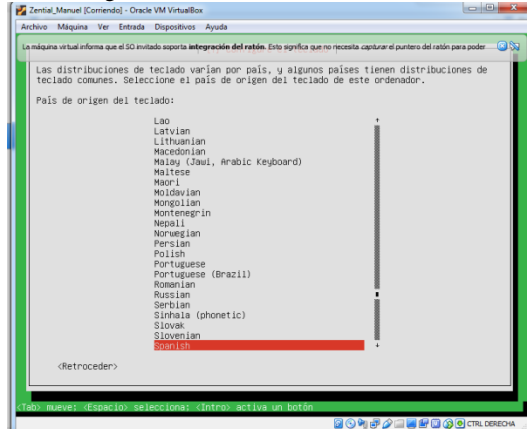


Imagen 5. Selección de caracteres especiales para el teclado

Empieza la instalación

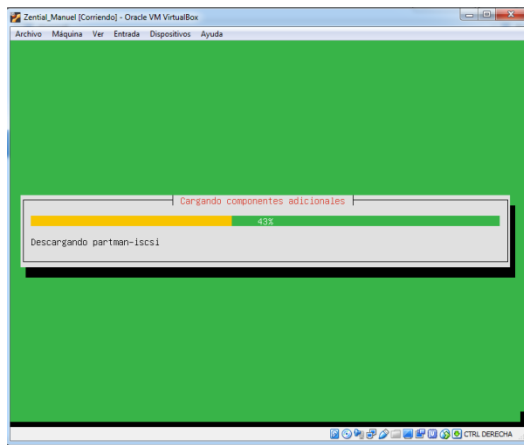


Imagen 6. Progreso de carga de datos para instalar

Le damos el nombre a la maquina

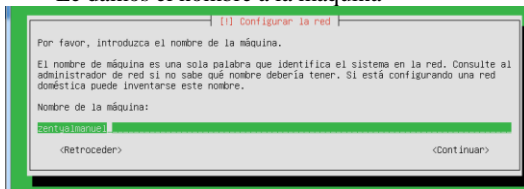


Imagen 7. Asignación de nombre para el Zentyal

Asignamos una contraseña para la cuenta antes creada e inicia la instalación.

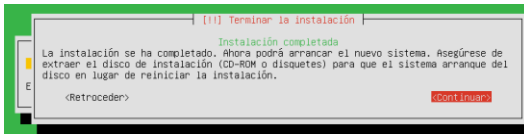


Imagen 8. Instalación terminada

El zentyal se inicia por primera vez e instalara paquetes adicionales como drivers de videos y paquetes de red adicionales



Imagen 9. Carga de componentes

2.4 Configuración inicial

Ingresamos con el usuario y la contraseña



Imagen 10. Logeo en Zentyal 6.0

Se ingresa el numero de activacion que nos dieron en el correo



Imagen 11. Activación de Software

En esta parte nos pide configurar las interfaces de Red



Imagen 12. Configuración interfaz de red

Seleccionamos los paquetes que vamos a utilizar

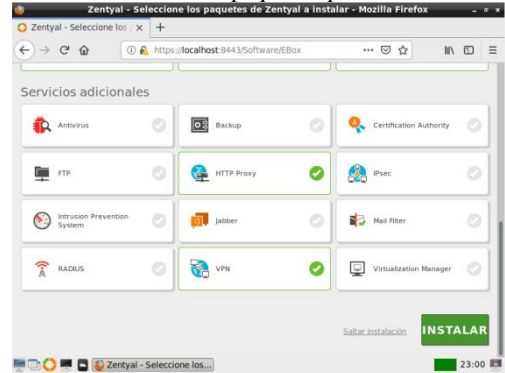


Imagen 13. Selección de paquete de servicios

Ahora pedira confirmación y comienza la instalación y se actualizan los paquetes



Imagen 14. Actualización de Software y paquetes

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

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.

Ingresamos en el icono de DHCP e damos en clic en el engranaje para iniciar la configuración.

Teniendo en cuenta la advertencia que nos arroja los sistemas nos dirigimos a los módulos y los activamos para su funcionamiento.

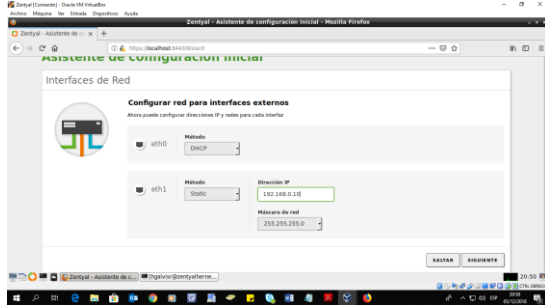


Imagen 15. Configuración de DHCP con las interfaces eth0 y eth1

Efectuamos scroll hacia abajo y visualizamos la configuración, los rangos de nuestra red, DNS.

Configuración DNS.



Imagen 16. Realizamos la configuración de los dns

Efectuamos configuración de rangos que deseamos.

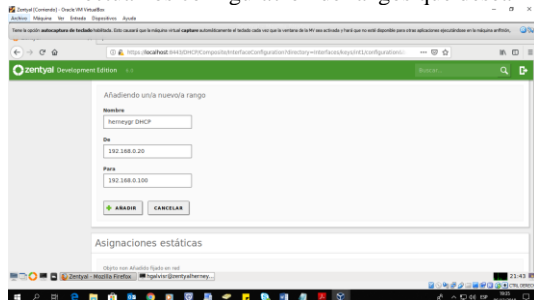


Imagen 17. Realicemos la configuración de los rangos

Rangos a utilizar.

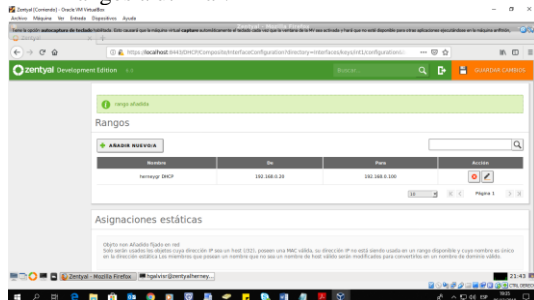


Imagen 18. Vista de configuración de los rangos

Pruebas servidor DHCP en Ubuntu Desktop. Evidencias uso servidor DHCP en Ubuntu desktop

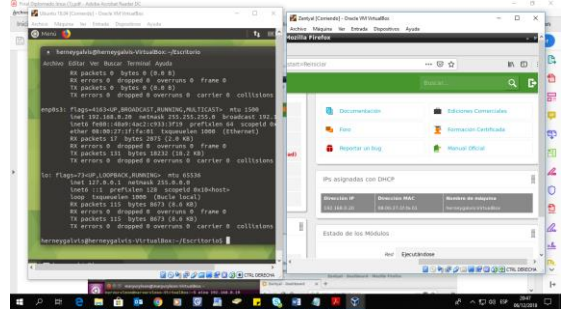


Imagen 19. Realicemos pruebas de conexión con nuestro servidor y la máquina de ubuntu

Evidencia al zentyal server con nombre de máquina, MAC e IP de Ubuntu desktop.

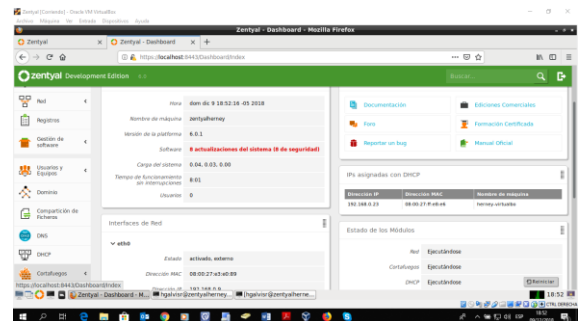


Imagen 20. Evidencia de conexión de nuestro equipo por DHCP al servidor zentyal

Se integra la configuración de DNS al servidor DHCP y se guardan los cambios.

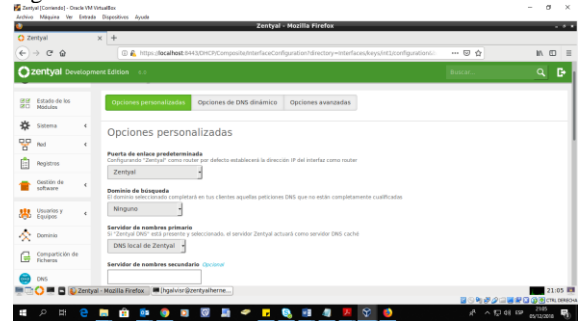


Imagen 21. Configuración de DNS al DHCP

Para la configuración del controlador de dominio se instala y se egresan los módulos como en los anteriores servicios.

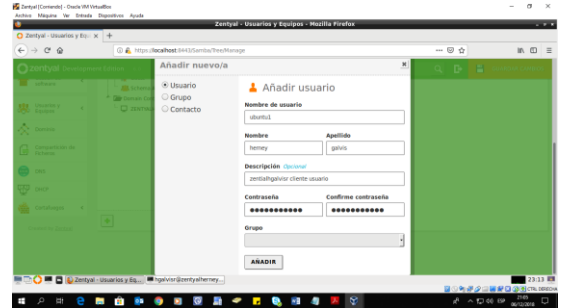


Imagen 22. Creación de usuario en el directorio activo zentyal

Añadimos y veremos cómo se ha creado el usuario

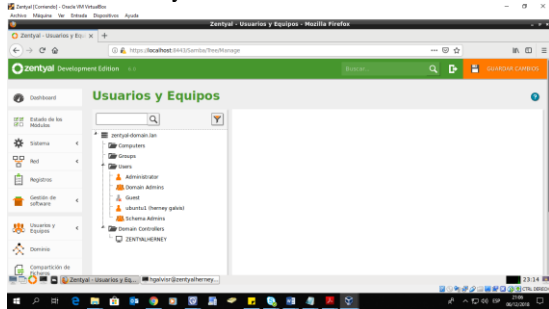


Imagen 23. Evidencia de creación de usuario en el dominio

Nos dirigimos a nuestra máquina de Ubuntu donde vamos a configurar /etc

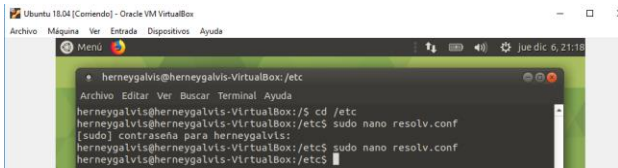


Imagen 24. Modificación del fichero /ETC

Abrimos nuestro fichero y modificamos nuestro nameserver

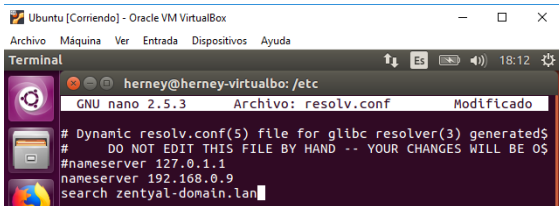


Imagen 25. Modificaciones de fichero

Para la Instalación del paquete likewiseopen, debemos hacer descargar de tres paquetes los cuales son:

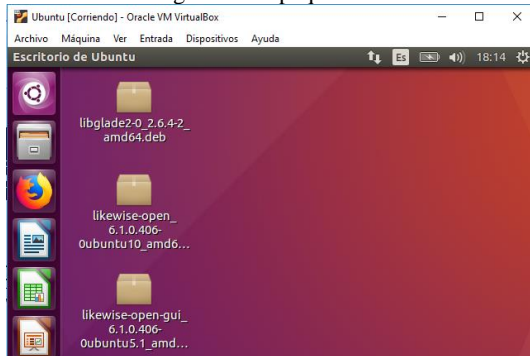


Imagen 26. Instaladores de de directorio activo

Una vez descargado debemos realizar la instalación de cada uno de los paquetes por medio de la terminal

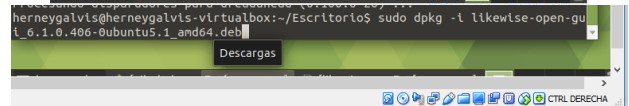
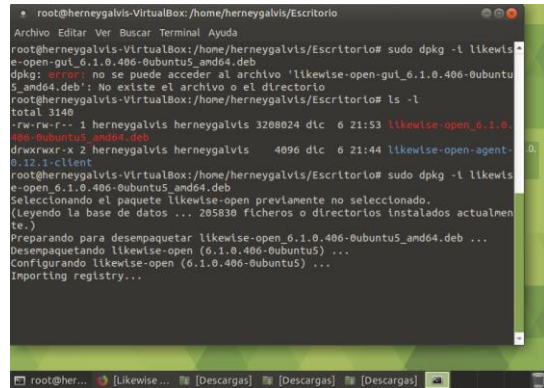


Imagen 27. Proceso de ejecución de los archivos likewiseopen

Una vez ejecutada los comandos de instalación procedemos a ingresar a modo grafico así: Sudo domainjoin-gui y nos abrirá una pantalla

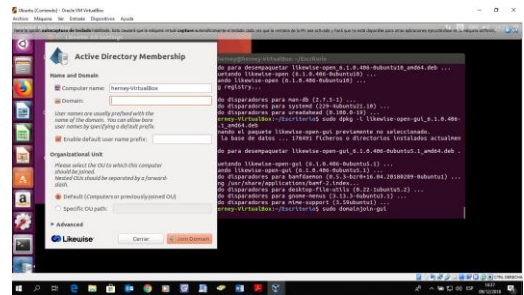


Imagen 28. modo grafico para ingresar el equipo al dominio antes creado

Ingresamos nuestro usuario y clave de dominio

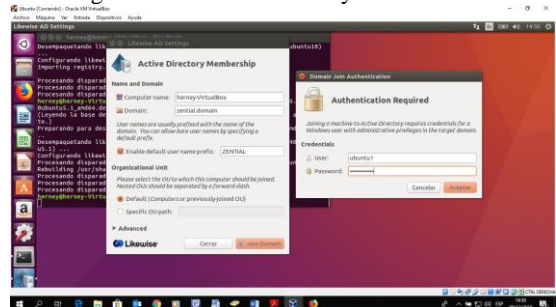


Imagen 29. Autenticacion de usuario y clave para ingreso al equipo al dominio

Despues de colocar nuestro usuario y clave esperaos a que el equipo se matricule en nuestro dominio

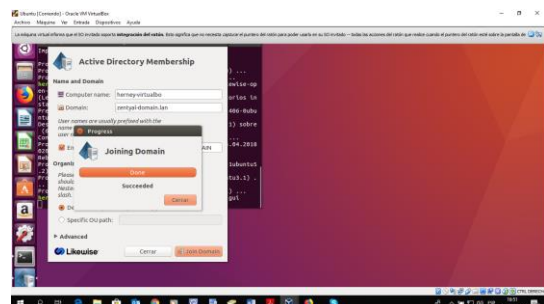


Imagen 30. Evidencia de acceso al dominio del equipo

Una vez ingresamos al dominio vamos al /etc para modificar la carpeta cd lightdm y vamos a modificar de la siguiente manera:

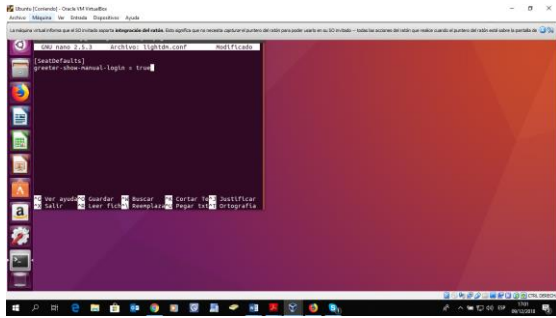


Imagen 31. Modificacion de fichero lightdm

Guardamos cambios y procedemos a reiniciar nuestra máquina virtual y aquí evidenciamos en nuestro servidor que la maquina ya están publicadas en nuestro directorio activo

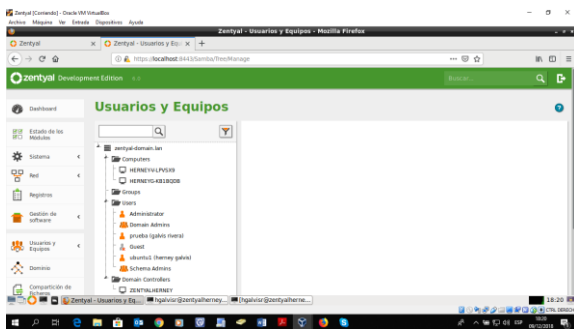


Imagen 32. Evidencia de registros de los equipos

Con todo esto proceso confirmamos que todo ha sido configurado de manera exitosa

IV. Temática 2 Proxy no transparente

Configuramos las tarjetas de las maquinas eth0 y eth1



Imagen 33. Configuración de tarjeta eth0

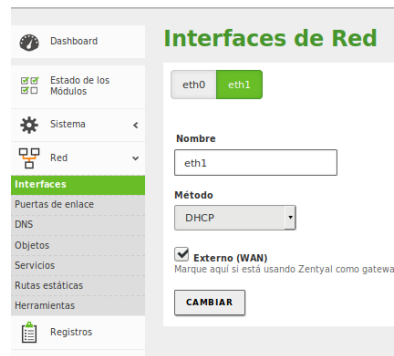


Imagen 34. Configuración de tarjeta eth1

Verificamos las puertas de enlaces que de por si quedan automáticamente ajustadas



Imagen 35. Interfaz puertas de enlace

Para verificar que tenemos conexión a internet para brindar el servicio debemos abrir una pestaña en el navegador y escribir una palabra en el buscador y el mostrara las opciones de búsqueda

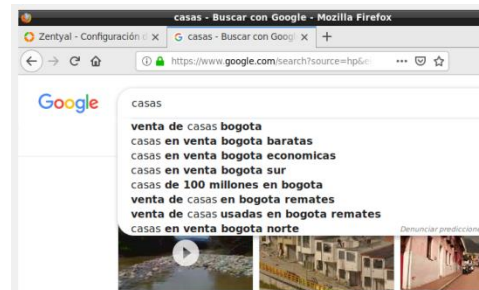


Imagen 36. Verificación conexión mozilla ubuntu

Y así verificamos que la conexión es válida

Luego debemos generar un rango en el cual nuestro servicio de DHCP pueda reconocer a los otros equipos y poderlos añadir al sistema, ingresamos al menú de la izquierda DHCP.



Imagen 37. Interfaz de tarjeta

Y damos clic al icono de la configuración, y la modificamos de modo que quede de esta manera

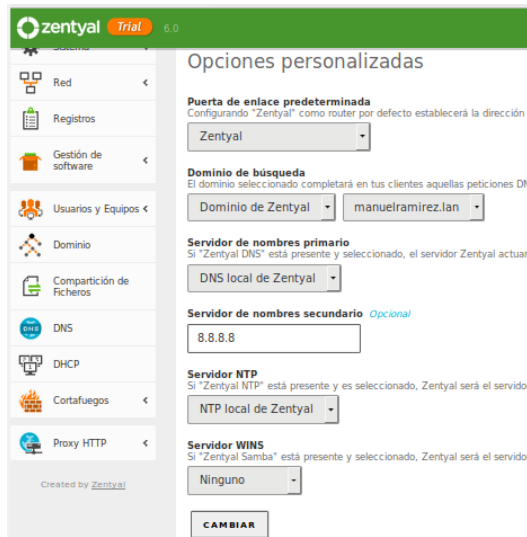


Imagen 38. Interfaz DHCP

Debemos configurar un rango es decir, decirle al Zentyal que reconozca las ip de equipos que lleguen al sistema, es decir cuando ustedes conecten una máquina virtual, Zentyal la reconocerá y automáticamente le asignara una ip dentro de ese rango, por el momento solo deben saber que Zentyal acoge a la máquina virtual de Ubuntu desktop y le cambia la ip normal y le pone la que está en el rango que vamos a configurar más abajo.

Nombre

De

Para

Imagen 39. Rangos modificados

Colocan un nombre que puede ser lo que ustedes quieran

Rangos

[+ AÑADIR NUEVO/A](#)

Nombre	De	Para	Acción
rangoA	10.10.10.50	10.10.10.100	

Página 1

Imagen 40. Verificacion de rangos en interfaz

Cuando configuramos las maquinas todas en el VirtualBox, asignamos unas tarjetas de red configuradas con adaptadores de tipo puente, pero debemos dejarlas de modo que Ubuntu y el Zentyal sean internas y Zentyal y el pc donde se instaló a máquina virtual sea externo

Ahora encendemos las máquinas virtuales primero el Zentyal y luego el Ubuntu

Luego en Zentyal entramos al dashboard y podremos apreciar que ya están conectados los equipos de manera automática

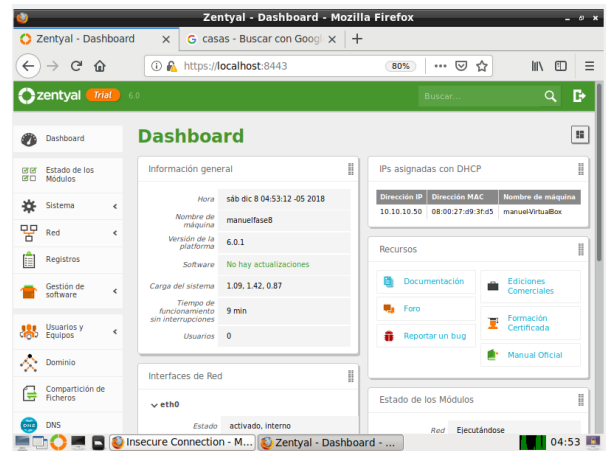


Imagen 41. Verificación conexión ubuntu en zentyal

IPs asignadas con DHCP

Dirección IP	Dirección MAC	Nombre de máquina
10.10.10.50	08:00:27:d9:3f:d5	manuelVirtualBox

Imagen 42. Interfaz conexión Ubuntu a Zentyal

Ingresamos al Ubuntu y para corroborar lo evidente hacemos un Ifconfig y automáticamente tendremos una ip distinta a la original

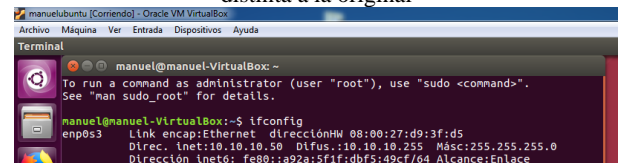


Imagen 43. Verificación IP Ubuntu

Ahora tenemos una ip dentro del rango que habíamos elegido y listo ya estaríamos enlazados

Para la Configuración de HTTP, Debemos ir al menú Proxy HTTP que está a la izquierda y desplegado encontraremos las reglas de acceso

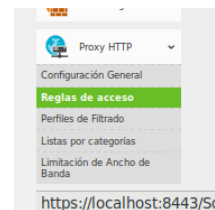


Imagen 44. Interfaz menú Proxy HTTP

Ingresaremos a la opción añadir nuevo y creare una regla que bloquee cualquier página a cualquier hora, esto permitirá más adelante corroborar que el navegador no puede acceder a ningún lado



Imagen 45. Interfaz reglas de acceso

Esta regla anterior bloqueara cualquier página y la opción quedara de la siguiente manera, si aparece el botón cambiar es porque yo ya la había creado si lo hacen desde cero, les aparecerá el botón añadir



Imagen 46. Verificación regla de acceso

Guardamos y vamos a Ubuntu a colocar una configuración adicional en el navegador, Configuraremos las opciones del navegador en la opción preferencias, luego en opciones

Primero configuraremos el proxy no transparente es decir que debemos nosotros mismos colocarlo

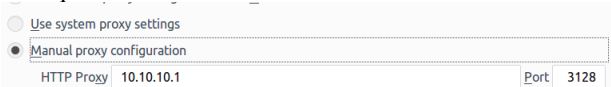


Imagen 47. Configuración de proxy Mozilla en Ubuntu

Adicional activaremos la opción de usar el proxy para todos los protocolos

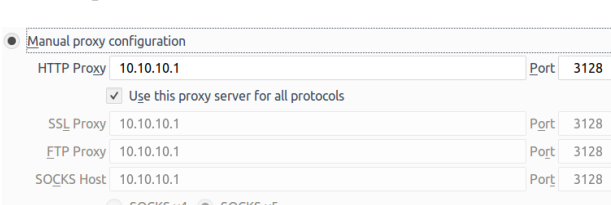


Imagen 48. Configuración de proxy protocolos Mozilla en Ubuntu

Ahora quitaremos las excepciones, el mismo Mozilla evita que el proxy se aplique para una dirección ip establecida y para el servername de dominio del Ubuntu, que normalmente sería Localhost y 127.0.0.



Imagen 49. Configuración de No proxy en Mozilla en Ubuntu

Acceptamos y ahora intentamos entrar a cualquier página que ustedes deseen y les pueden aparecer dos cosas

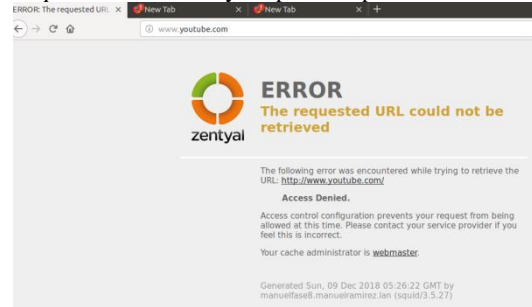


Imagen 50. Verificación de regla de bloqueo desde Zentao 2

Ya con esto sabemos que el sistema está funcionando, si lo que deseamos es que el servicio de internet regrese solo debemos cambiar la opción de acceso en las reglas de acceso y vamos a editarlas

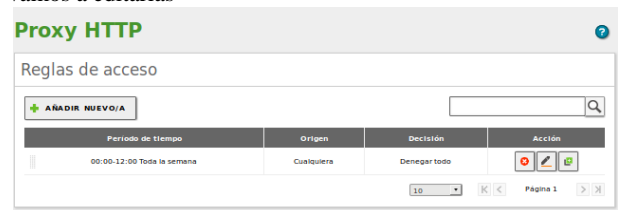


Imagen 51. Interfaz Proxy HTTP 2

Lo que nos permitirá modificar como lo vimos anteriormente, pero en vez de denegar vamos a permitir todo

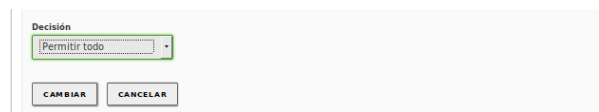


Imagen 52. Verificación de regla de acceso 2

Ahora guardamos y vamos a Ubuntu a ver si las reglas fueron aceptadas

Y veremos que ahora Mozilla acepta todo

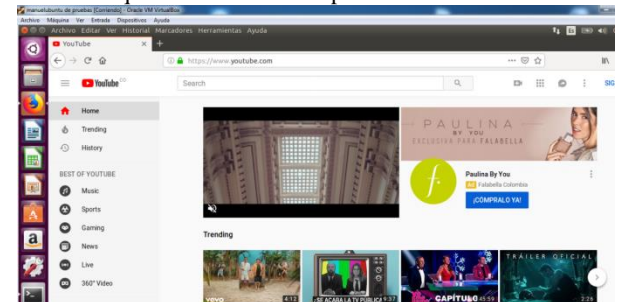


Imagen 53. Verificación de regla de acceso en Mozilla Ubuntu

Y con esto damos por terminado el proceso de la temática número 2.

V. Temática 3 Cortafuegos

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

En primer lugar, realizamos la instalación de los paquetes necesarios y el cortafuegos al configurar Zentyal.

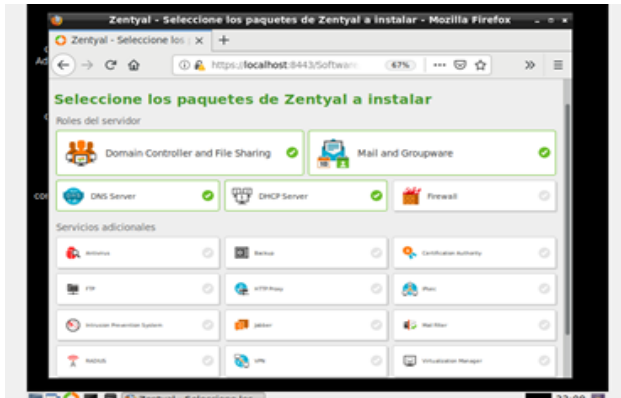


Imagen 54. Selección de paquetes

Configuramos la red al terminar la instalación elegimos cual es la tarjeta externa e interna, en mi caso elegí eth0 para externa y eth1 interna

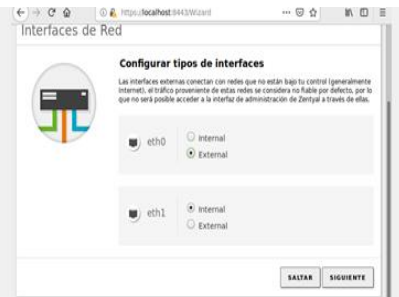


Imagen 55. Interfaz de red

Luego le asignamos la dirección IP a la tarjeta interna la cual será la puerta de enlace de los equipos de la red local que están conectados

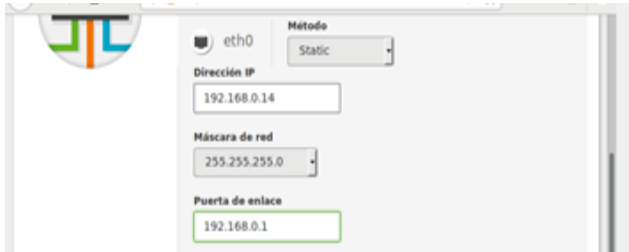


Imagen 56. Asignación dirección IP

En la primera tarjeta ponemos el método DHCP y marcamos la casilla externa (WAN) que es la conexión a internet.



Imagen 57. Interfaz de red externa

Y en la segunda colocamos el método estático y la dirección IP que va a utilizar el equipo.

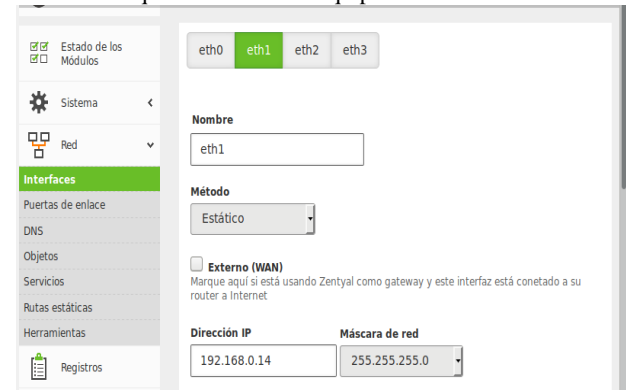


Imagen 58. Interfaz de red interna

Una vez configurado la red vamos al firewall para crear una regla de filtrado.



Imagen 59. Selección de cortafuegos

Damos clic en cortafuegos y seleccionamos reglas de filtrado para redes internas configurar reglas



Imagen 60. Selección de reglas de filtrado

Damos clic en añadir nueva regla para crear la regla



Imagen 61. Añadir nueva regla

Antes de agregar la regla buscamos la dirección IP de la web que vamos a bloquear, en la terminal ejecutamos el comando ping seguido del dominio.

```
victorurrego@victorurrego-victorurrego:~$ ping facebook.com
ping: Facebook.com (157.240.6.35): 56(84) bytes of data:
64 bytes from edge-star-mnl-shv-01-bog1.facebook.com (157.240.6.35): icmp_seq=1
ttl=58 time=43.9 ms
64 bytes from edge-star-mnl-shv-01-bog1.facebook.com (157.240.6.35): icmp_seq=2
ttl=58 time=42.9 ms
64 bytes from edge-star-mnl-shv-01-bog1.facebook.com (157.240.6.35): icmp_seq=3
ttl=58 time=42.7 ms
64 bytes from edge-star-mnl-shv-01-bog1.facebook.com (157.240.6.35): icmp_seq=4
ttl=58 time=43.9 ms
64 bytes from edge-star-mnl-shv-01-bog1.facebook.com (157.240.6.35): icmp_seq=5
ttl=58 time=42.4 ms
64 bytes from edge-star-mnl-shv-01-bog1.facebook.com (157.240.6.35): icmp_seq=6
ttl=58 time=43.7 ms
^C
```

Imagen 62. Identificación IP dominio Facebook

En esta editamos la regla añadimos la opción de denegar o permitir la conexión, agregamos el origen, si queremos lo podemos aplicar a un solo equipo de la red o a todos, en destino colocamos la dirección del dominio que queremos bloquear, por último, colocamos el servicio que vamos a bloquear.

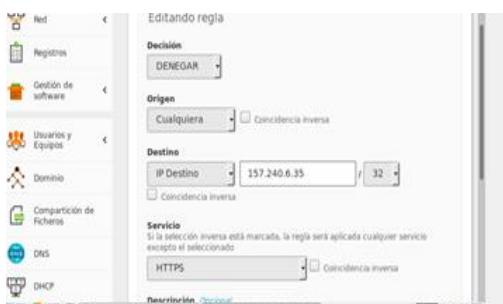


Imagen 63. Edición de regla

Colocamos la descripción con el nombre del sitio a bloquear



Imagen 64. Configuración de la regla

Quedando la regla así y al finalizar damos en guardar en el disco que nos aparece en la parte superior de la página



Imagen 65. Regla agregada.

En la imagen podemos ver que tenemos el equipo con Ubuntu registrado en la red.



Imagen 66. Identificación equipo Ubuntu en la red de central

Acá podemos ver que nuestra máquina Ubuntu está conectada a Zentyal y que la web Facebook funciona antes de haberle aplicado la regla de denegar servicio.

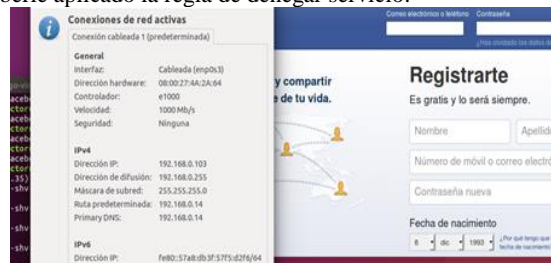


Imagen 67. Vista del equipo Ubuntu conectado a la red con Zentyal

Aplicando la regla la página de Facebook ya no funciona entonces se ha configurado con éxito el cortafuego para el bloqueo de páginas web



Imagen 68. Vista del bloqueo del dominio Facebook

Con esta parte finalizamos esta temática.



Imagen 69. Comprobación del equipo está conectada a la red Zentyal

VI. Temática 4 File Server y Print Server

Primero vamos a la opción "Dominio", vamos a encontrar los datos registrados de nuestro dominio de red, se chequea "habilitar perfiles móviles", Letra de unidad "H" y debe quedar como está en la imagen, clic en cambiar y guardar.

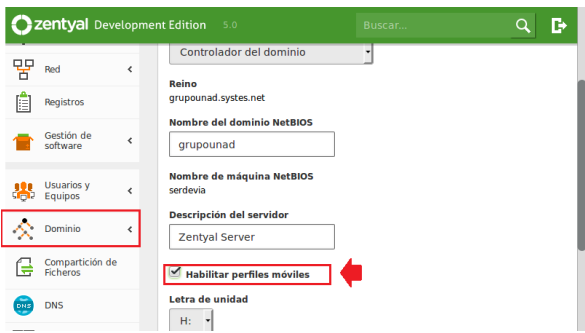


Imagen 69. Menú Dominio desde Zentyal

Luego iniciamos nuestra máquina Ubuntu Dsktop, y verificamos la dirección asignada por la red. Importante que la tarjeta de red de la máquina quede en “Adaptador 1” como “red Interna”, en la imagen tenemos IP 192.168.1.151.

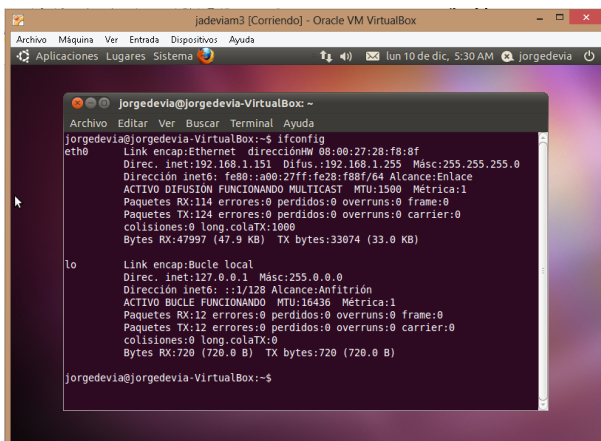


Imagen 70. Terminal de Ubuntu Desktop con comando ifconfig

Adicionalmente nuestro servidor de dominio ya registra nuestra máquina Ubuntu, de esta forma confirmamos que la máquina está conectada a nuestra red.



Imagen 71. Vista de registro de conexión por DHCP

Desde la opción de “usuarios y grupos” se crea un nuevo registro.



Imagen 72. Vista formulario para crear usuario

Luego creamos un nuevo grupo llamado “Administrativos”, clic en “añadir”

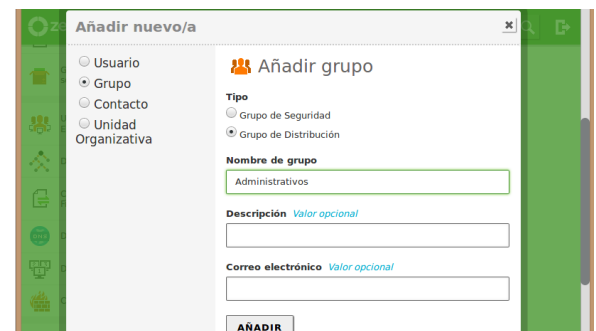


Imagen 73. Vista formulario para crear grupo

Luego incluimos a nuestro usuario “Iamorocho” al grupo “Administrativo”, hacemos clic en el símbolo “+” y luego guardamos los cambios.

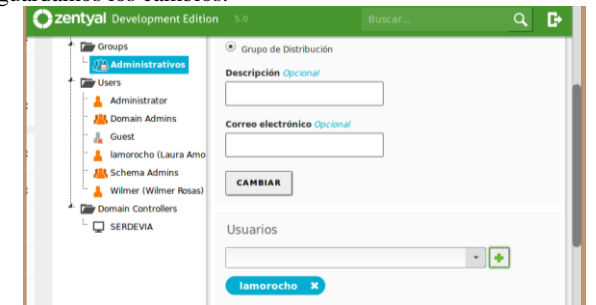


Imagen 74. Imagen inclusión de usuario a grupo

Compartir Ficheros y Directorios

Vamos a la opción “Compartición de Ficheros” y hacemos clic en “Añadir Nuevo”



Imagen 75. Vista para añadir fichero desde Zentyal

Debemos chequear la casilla de “Habilitado” para que los usuarios de la red puedan acceder a los recursos compartidos, adicionalmente registramos la información del nombre del recurso, Ruta y clic en “añadir”.

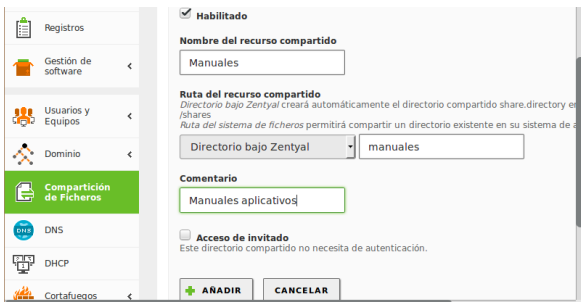


Imagen 76. Vista creando fichero

En esta imagen ya podemos evidenciar la creación del recurso, ahora debemos configurar los permisos, hacemos clic en la opción de “Control de acceso”.



Imagen 77. Vista con Botón para control de acceso

Hacemos clic en “Añadir” para configurar que usuarios tendrán acceso y de que tipo.



Imagen 78. Vista botón para añadir permisos de usuario

Se puede habilitar permisos de “Lectura y Escritura”, de solo lectura o escritura o ninguno.



Imagen 79. Imagen configurando permisos

Finalizada la configuración del directorio y sus permisos, vamos a nuestra máquina Ubuntu e iniciamos sesión con el usuario “lamoroch”, y evidenciamos que tiene permisos para entrar a la carpeta del Administrador.

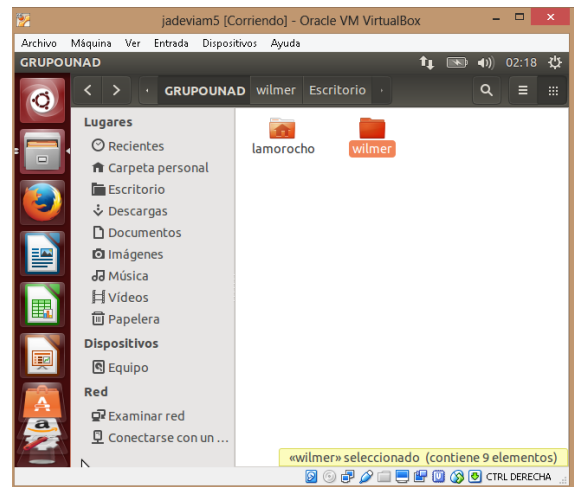


Imagen 80. Vista validando el acceso a recursos

Desde la opción “conectar a servidor” podemos ubicar la ruta de nuestro recurso compartido.

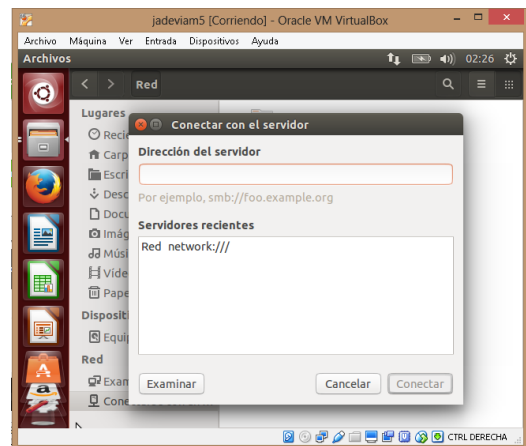


Imagen 81. Vista validando el acceso a recursos

VII. Temática 5 VPN

Las siglas VPN provienen del término en inglés Virtual Private Network, lo que en español significa: red virtual privada.

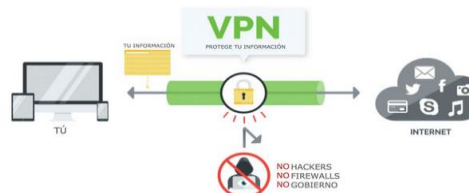


Imagen 82 ejemplo de una vpn

Con la conexión VPN, podemos establecer contacto con aparatos que estén alojadas en nuestra red local u otras redes locales de forma totalmente segura, ya que esta conexión se establece entre ambas máquinas viajan totalmente cifradas.

OpenVPN posee las siguientes ventajas:

- Autenticación mediante infraestructura de clave pública.
- Cifrado basado en tecnología SSL.
- Clientes disponibles para Windows, Mac OS y Linux.
- Más sencillo de instalar, configurar y mantener que IPSec, otra alternativa para VPNs en software libre.
- Posibilidad de usar programas de red de forma transparente.

CONFIGURACIÓN DE LA VPN

Ingresamos a Linux Zentyal y seleccionamos autoridad de certificación. En el cual realizamos la configuración del ciclo de vida de los certificados expedidos por esta.

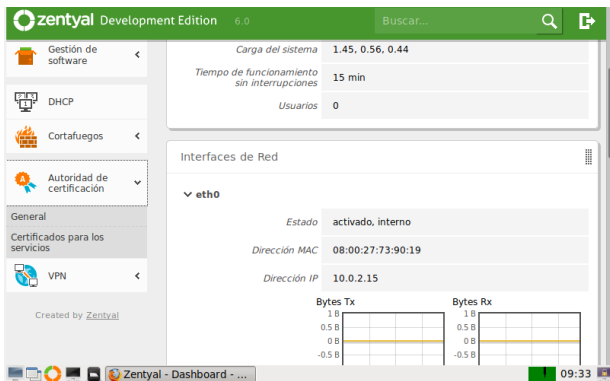


Imagen 83 Autoridad de Certificación.

Nos ubicamos en general y creamos el certificado de la autoridad ingresamos el nombre y los días ha expirar.

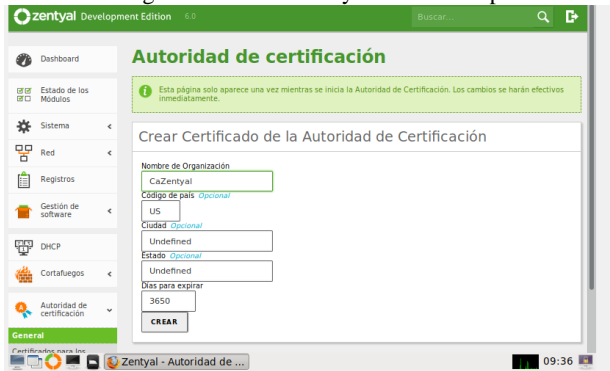


Imagen 84 Creación de certificado.

Seleccionamos la opción VPN / servidores y procedemos a crear el servidor VPN el cual nos escuchara todas la interfaces externas.



Imagen 85 Creación de servidor VPN.

Verificamos la lista de servidores es decir yo puedo crear varios tipos de servidores para una empresa.

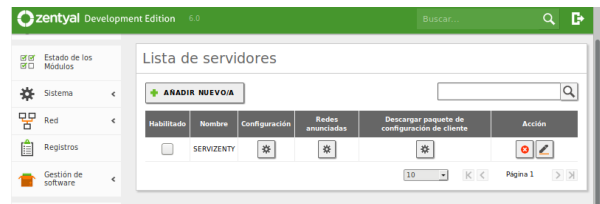


Imagen 86 Configuración de servidor VPN.

En el botón de configuración procedemos a realizar la configuración del puerto ya se UDP o TCP, dirección del servidor VPN, certificado y tipos de conexión.

(TCP) Transmission-Control-Protocol, en español Protocolo de Control de Transmisión es de los protocolos fundamentales en Internet. (UDP) Es un protocolo del nivel de transporte basado en el intercambio de datagramas. Permite el envío de datagramas a través de la red sin que se haya establecido previamente una conexión, ya que el propio datagrama incorpora suficiente información de direccionamiento en su cabecera.



Imagen 87 Configuración del servidor VPN.

Ingresamos a Red / servicios en cual creamos nuestro servicio de VPN

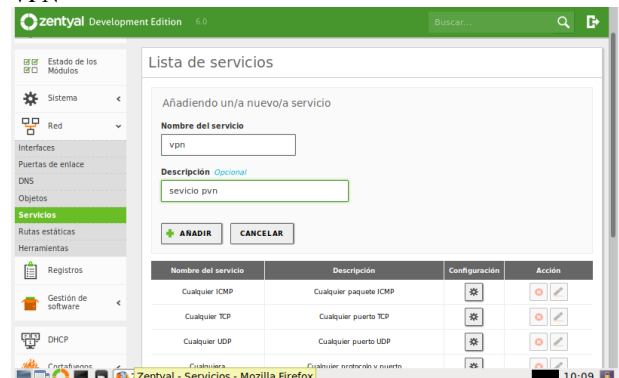


Imagen 88 Creación del servicio.

Procedemos a configurar el servicio como lo es el protocolo, puerto origen y el puerto que en nuestro caso es 1194

El puerto TCP 1194 usa el Protocolo de Control de Transmisión. TCP es uno de los protocolos principales en redes TCP/IP. TCP es un protocolo orientado en la conexión, necesita el apretón de manos para determinar comunicaciones de principio a fin. Solo cuando la conexión es determinada, los

datos del usuario pueden ser mandados de modo bidireccional por la conexión.



Imagen 89 Configuración del servicio

Ingresamos a cortafuegos y escogemos filtrado de paquetes.

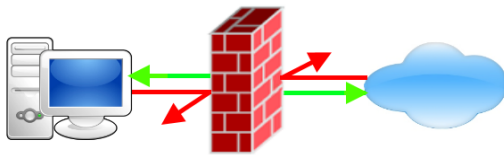


Imagen 90 Ejemplo de cortafuegos o firewall

Un cortafuego o (firewall) es una parte de un sistema o una red que está diseñada para bloquear el acceso no autorizado, permitiendo al mismo tiempo comunicaciones autorizadas.



Imagen 91 Cortafuegos

En el filtrado de paquetes procedemos a crear cada una de las reglas que necesitemos para nuestra conexión como lo es la decisión el origen y el servicio



Imagen 92 Configuración de cortafuegos

Procedemos a realizar la configuración del paquete de configuración de clientes. Tipo de cliente en este caso Linux, certificado e cliente, estrategia de conexión, dirección del servidor



Imagen 93 Configuración de paquete de cliente

Descargamos los certificados del equipo cliente

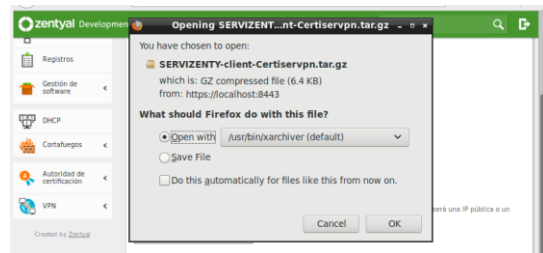


Imagen 94 Descarga del paquete cliente.

En el equipo cliente (ubuntu) procedemos a realizar la instalación de openvpn.

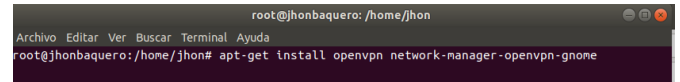


Imagen 95 Instalación de openvpn

Ingresamos a red en cual nos trae la opción de vpn allí procedemos a realizar la importación del archivo q descargamos de la creación del servidor Zentyal

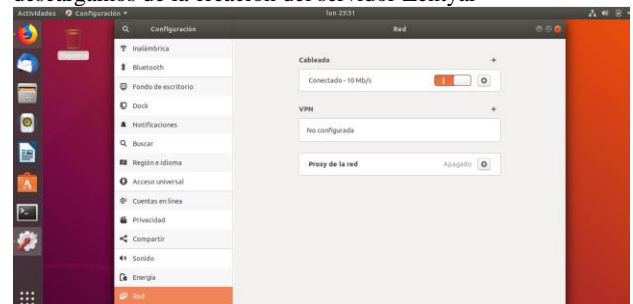


Imagen 96 Configuración de vpn

Archivo que importamos en VPN

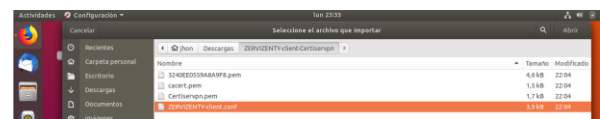


Imagen 97 Archivos a importar

Archivos importados en la configuración



Imagen 98 Archivos importados

Verificamos las pruebas de conexión en el servidor zentyal.

Fecha	Evento	Daemon	Tipo	IP remoto	Certificado remoto
2018-12-10 23:37:13	Conexión a cliente iniciada	ZERVIZENTY	server	192.168.0.6	Certisengn
2018-12-10 23:35:20	Conexión a cliente iniciada	ZERVIZENTY	server	192.168.0.6	Certisengn

Página 1



Imagen 99 Prueba de conexión entre linux ubuntu y zentyal

Conclusiones

✓ Se logró instalar y configurar GNU/Linux Zentyal Server 5.0 con entorno gráfico, como base para implementar los servicios requeridos

✓ Se configuraron dos interfaces de red: eth0 y eth1 estableciendo conexión NAT y conexión interna respectivamente.

✓ Se configuraron los paquetes DHCP Server, DNS Server y Controlador de Dominio sobre Zentyal

✓ Se configuró el acceso de una estación de trabajo GNU/Linux Ubuntu Desktop a través de la creación de un usuario asociado a un grupo de distribución.

✓ Mediante esta actividad se instala y se configura la plataforma Zentyal que usa el servidor web Apache y soporta Email, calendarios, contactos, antivirus, antispam y se sincroniza con dispositivos móviles. Incluye controlador de dominio y servicio de directorio, servicios básicos de redes y cortafuegos

✓ Para esta actividad se logró significativamente la conexión Vpn entre Zentyal y Windows con todas sus configuraciones correctamente, se aprendió sobre la importancia del manejo de conexiones seguras en el caso planteado y esta solución será un éxito para la empresa.

✓ Se identificó las principales características de la distribución GNU/Linux Zentyal, donde podemos utilizar esta herramienta con múltiples características DNS, DHCP, Firewall, Proxy, Red.

✓ La configuración por proxy mediante Zentyal se debe realizar con la dirección ip del mismo servidor, para que nos sirva como gateway en las conexiones a internet mediante el puerto que deseemos configurar.

✓ Como Proxy con Zentyal podemos configurar reglas de acceso con tiempos diferentes, intervenir el ancho de banda del canal de internet que estemos utilizando, adicional de dar tazas de navegación a nuestros usuarios.

Referencias

[1] Josep, J. E., & Remo, S. B. (2007). Administración avanzada de GNU/Linux. Universitat Oberta de Catalunya – UOC. Recuperado de <http://hdl.handle.net/10609/226>

[2] Béjar, H. M. D. L. C. (2015). Selección, instalación, configuración y administración de los servidores de transferencia de archivos (UF1275). Madrid, ES: IC Editorial. Retrieved from <http://bibliotecavirtual.unad.edu.co:2077/lib/unadsp/reader.action?ppg=150&docID=11148772&tm=1480301043772>

[3] Zentyal Wiki. (2015). Instalación y configuración de Zentyal Server 5. Recuperado de: [https://wiki.zentyal.org/wiki/Es/4.1/Servicio_de_resolucion_de_nombres_de_dominio_\(DNS\)](https://wiki.zentyal.org/wiki/Es/4.1/Servicio_de_resolucion_de_nombres_de_dominio_(DNS))

[4] Zentyal Wiki. (2015). Instalación y configuración de Zentyal Server 5. Recuperado de: [https://wiki.zentyal.org/wiki/Es/4.1/Servicio_de_resolucion_de_nombres_de_dominio_\(DNS\)](https://wiki.zentyal.org/wiki/Es/4.1/Servicio_de_resolucion_de_nombres_de_dominio_(DNS))

[5] Zentyal Wiki. (2015). Instalación y configuración de Zentyal Server 5. Recuperado de: [https://wiki.zentyal.org/wiki/Es/3.5/Servicio_de_redes_privadas_virtuales_\(VPN\)_con_OpenVPN](https://wiki.zentyal.org/wiki/Es/3.5/Servicio_de_redes_privadas_virtuales_(VPN)_con_OpenVPN)

[6] Configurar cliente OpenVPN Linux <https://nebul4ck.wordpress.com/2016/07/10/configurar-cliente-openvpn-linux/>