

Solucionando necesidades específicas con GNU/Linux

Edison F. Jiménez C, Camilo Esteban Martínez Avila, Miguel Suescun, Andrés Mauricio Triana Reina y Fredy Andrés Villamizar.

*Escuela de Ciencias Básicas Tecnología e Ingeniería, UNAD
Bogotá, Colombia*

edijim@hotmail.es

silayes@hotmail.com

debian789@gmail.com

andrestrianareina@outlook.com

andres_villamizar@hotmail.com

Abstract— En el presente documento se desarrollará la implementación de soluciones tecnológicas TIC, para red de computadores, basados en la distribución Zentyal 6.0. Esta distribución es una alternativa, en modo de ejecución gráfica, a los tradicionales servidores GNU/Linux y Windows Server de una infraestructura de red de telecomunicaciones.

I. INTRODUCCIÓN

En las últimas décadas GNU/Linux a dado para todo tipo de variantes. Zentyal es un derivado de Ubuntu que permite configurar toda la infraestructura de red de una forma gráfica y cómoda para el administrador; su falencia o ventaja, todo depende del punto de vista, es de pago y trae soporte. Mediante una intuitiva interfaz y configuración automática de las características se vuelve una alternativa más a las estudiadas durante los procesos formativos en Ingeniería de sistemas.

II. INSTALACIÓN ZENTYAL

Zentyal al estar basado en Ubuntu server, su instalación es parecida a dicha distribución y funciona sobre arquitecturas estándar x86 (32-bit) o x86_64 (64-bit). Los requerimientos de hardware para un servidor Zentyal dependen de los módulos que se instalen, de cuántos usuarios utilizan los servicios y de sus hábitos de uso. Con el fin de tener una instalación correcta, se debe seleccionar el tipo de red puente, para poder conectarse a las demás máquinas que estén disponibles en la red



Fig. I Configuración interface de red máquina virtual.

En la instalación se debe seleccionar el nombre del usuario y

su respectiva contraseña:



Fig. II Nombre de la máquina

Instalación finalizada de la máquina



Fig. III Aceptar riesgos de funcionamiento en el navegador

Una vez ingresamos estemos en la máquina, debemos ingresar a la dirección <https://localhost:8443>, donde debemos aceptar en el navegador los riesgos de entrar a este tipos de entornos

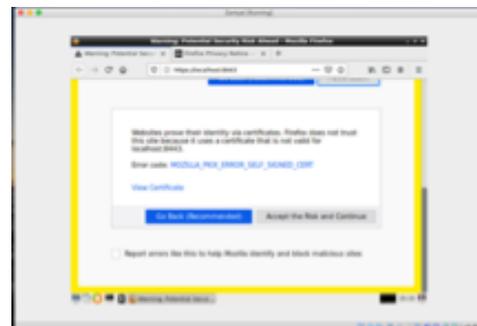


Fig. IV Aceptar riesgos de funcionamiento en el navegador

Con este proceso realizado, debemos ingresar con el usuario y contraseña creado al momento de instalación



Fig. V Inicio de sesión Zentyal Server

III. DNS, DHCP Y CONTROLADOR DOMINIO

El Sistema de Nombres de Dominio o DNS es un sistema de nomenclatura jerárquico que se ocupa de la administración del espacio de nombres de dominio (Domain Name Space). Su labor primordial consiste en resolver las peticiones de asignación de nombres. Esta función se podría explicar mediante una comparación con un servicio telefónico de información que dispone de datos de contacto actuales y los facilita cuando alguien los solicita. El DHCP es una extensión del protocolo Bootstrap (BOOTP) desarrollado en 1985 para conectar dispositivos como terminales y estaciones de trabajo sin disco duro con un Bootserver, del cual reciben su sistema operativo. El DHCP se desarrolló como solución para redes de gran envergadura y ordenadores portátiles y por ello complementa a BOOTP, entre otras cosas, por su capacidad para asignar automáticamente direcciones de red reutilizables y por la existencia de posibilidades de configuración adicionales. Un Directorio Activo (AD) es un servicio de directorio para su uso en un entorno Windows o Linux Server. Se trata de una estructura de base de datos distribuida y jerárquica que comparte información de infraestructura para localizar, proteger, administrar y organizar los recursos del equipo y de la red, como archivos, usuarios, grupos, periféricos y dispositivos de red.

A. Instalación de Roles DNS, DHCP y Directorio Activo

Ingresamos a la consola de administración Para ejecutar los primeros pasos, ingresamos con el usuario que hemos creado en la instalación.



Fig. VI configuración inicial

Seleccionamos el rol del servidor, dando click en cada uno de ellos, en nuestro caso seleccionamos Domanin Controller, DNS y DHCP

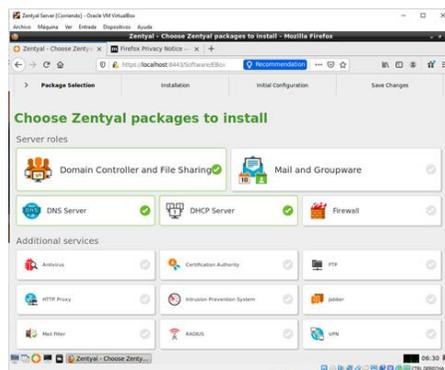


Fig. VII Paquetes de instalación

Luego damos click en el botón Install



Fig. VII instalar

Confirmamos que vamos a instalar estos paquetes.

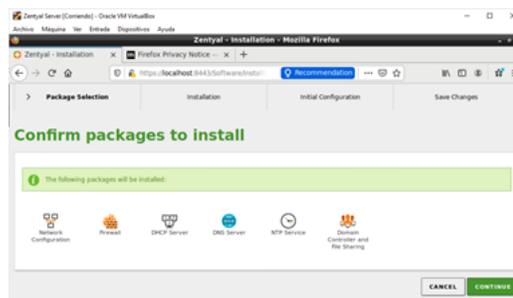


Fig. VII confirmación de paquetes

Inicia nuestro proceso de instalación de roles.

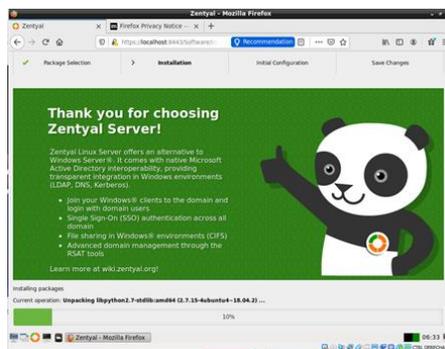


Fig. IX progreso de instalación

Ahora debemos realizar la configuración de los roles que hemos definidos para nuestro servidor. Definimos el tipo de interfaz de red, en nuestro caso la definimos como interna.

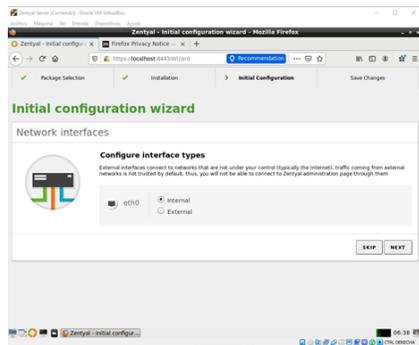


Fig. X configuración interface de red

Ingresamos los valores para nuestra tarjeta de red, es importante que en la opción de domain name server 1, dejemos la misma ip que estamos configurando para poder configurar el DNS

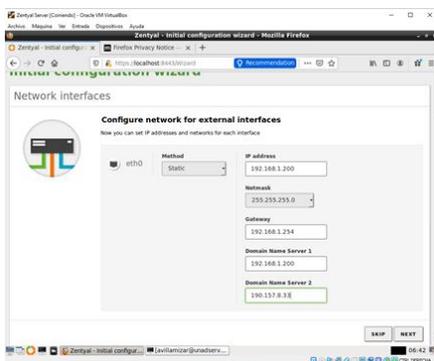


Fig. XI configuración interface de red

Indicamos el tipo de servidor, en nuestro caso seleccionamos Standalone Server, ya que es nuestro primer servidor de dominio, si ya tuvieses un servidor de dominio, debemos darle la opción adicional, ingresamos el nombre de nuestro dominio

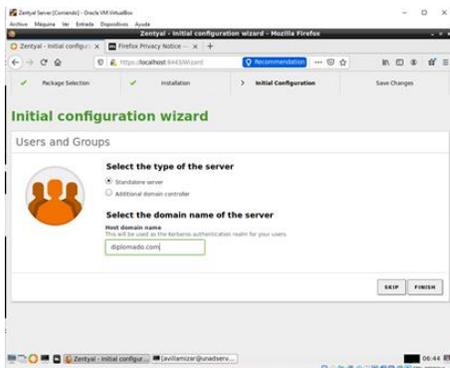


Fig. XII configuración del servidor

Nos genera una advertencia que indica que va a cambiar el nombre. Damos click en OK.

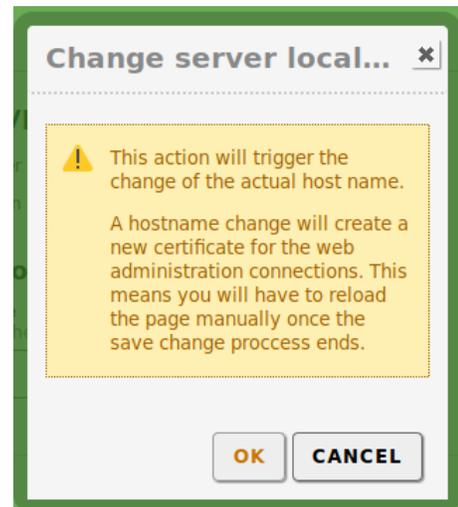


Fig. XIII Confirmación de configuración

Se guardan los cambios en los módulos y de esta forma hemos configurado inicialmente los roles de nuestro servidor

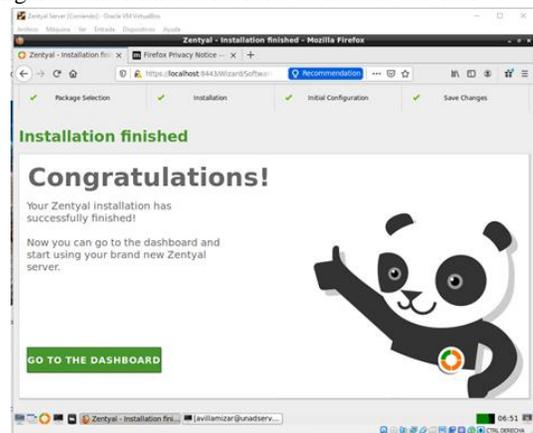


Fig. XIV finalización de configuración

B. Configuración de Roles DNS, DHCP y Directorio Activo

Procedemos a configurar el rol del servidor DHCP

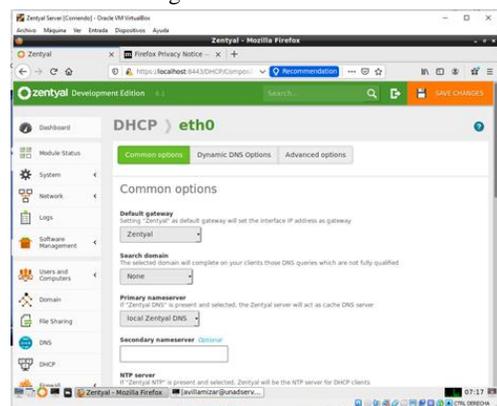


Fig. XV configuración rol DHCP

Definimos el rango para las estaciones clientes

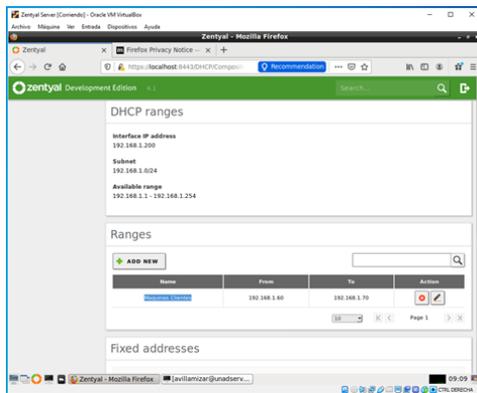


Fig. XVI definición de los rangos

Importante guardar los cambios

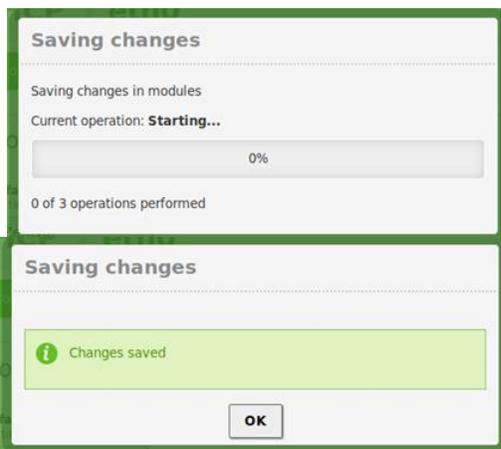


Fig. XVII cambios guardados

Creamos un usuario en la consola de Zentyal con el cual podamos ingresar a nuestro sistema

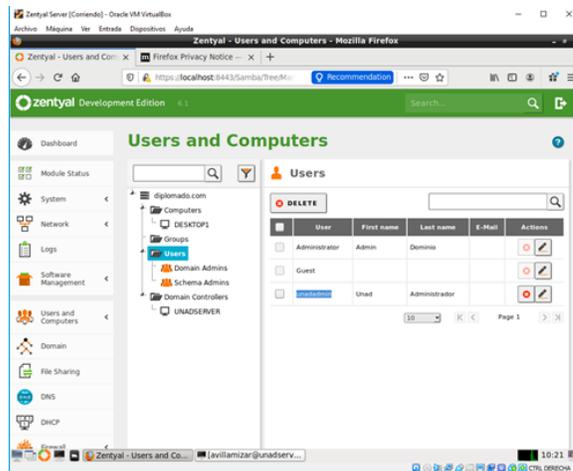
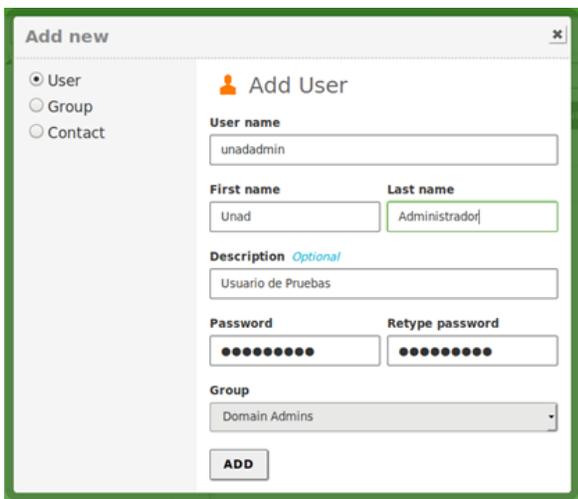


Fig. XVIII creación de usuario

C. Incluir Máquina cliente al Dominio

En la máquina Ubuntu revisamos el rango de direccionamiento IP, vemos que como es la primera máquina cliente nos toma la IP 192.168.1.60 y que este activo la opción de DHCP Automático

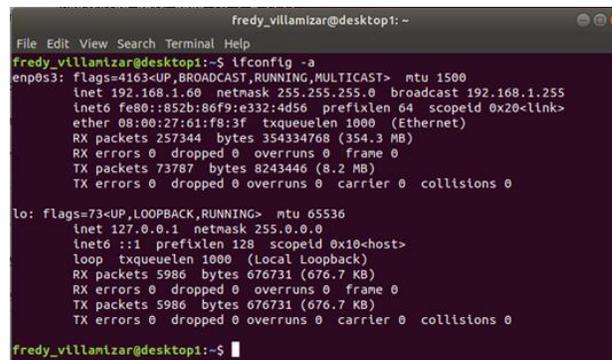


Fig. XIX verificación de la dirección IP

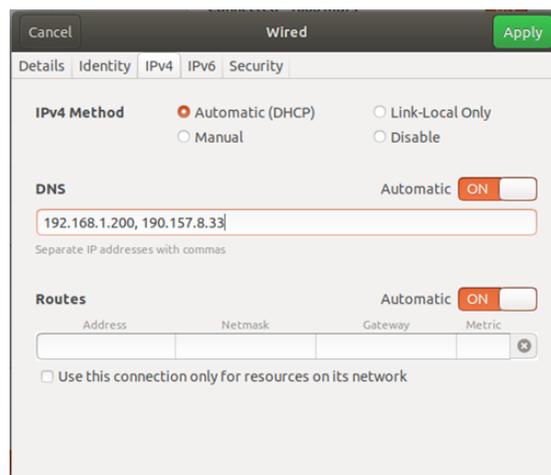


Fig. XX verificación de la dirección IP

Para incluir una maquina Ubuntu Desktop al Dominio, debemos ingresar en la máquina y descargar una herramienta

que nos permitirá realizar la conexión.

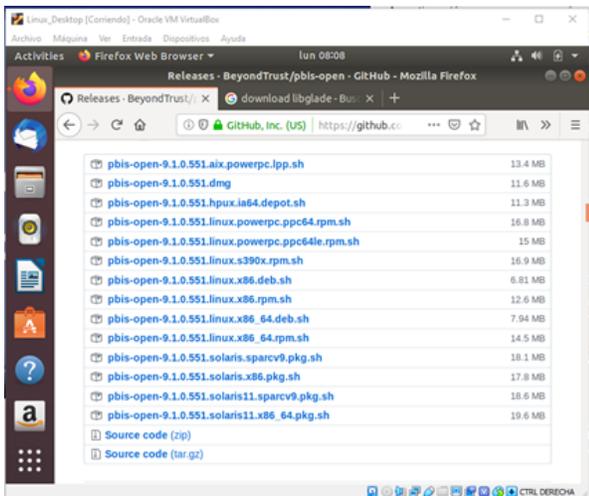


Fig. XXI indicando el dominio

Para mi máquina que es de 64 bits descargo la siguiente versión:



Fig. XXII descargar la versión

Una vez descargado en el sistema le doy al archivo permisos de ejecución y lo ejecuté

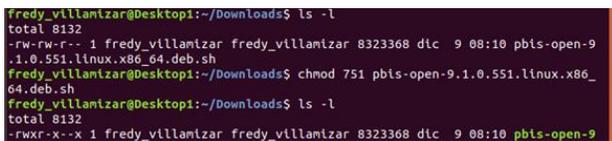


Fig. XXIII ejecución del archivo

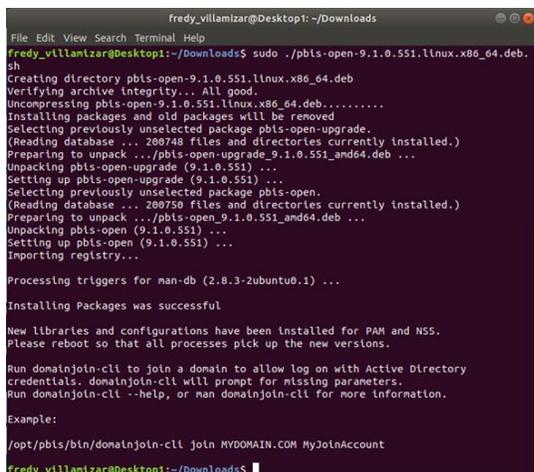


Fig. XXIV ejecución del archivo

Una vez instalado el software pbis-open tendré la oportunidad de unirse a dominio como me indica la propia aplicación



Fig. XXV indicar el dominio

Ahora bien, la máquina está unida a dominio, pero hemos de activar la capacidad en el cliente de escribir el usuario de dominio para iniciar sesión.

Editamos el siguiente fichero:



Fig. XXVI edición fichero

Incluimos la línea inferior para hacer un login manual.

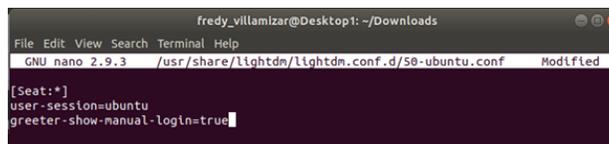


Fig. XXVII edición fichero

Finalmente asignamos un shell al usuario que entre a través de la configuración del pbis-open (los usuarios de dominio)

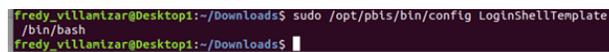


Fig. XXVIII modificación shell

Una vez hecho esto, y después de reiniciar el sistema, en la consola de Zentyal vemos ya nuestro computador agregado bajo el dominio.

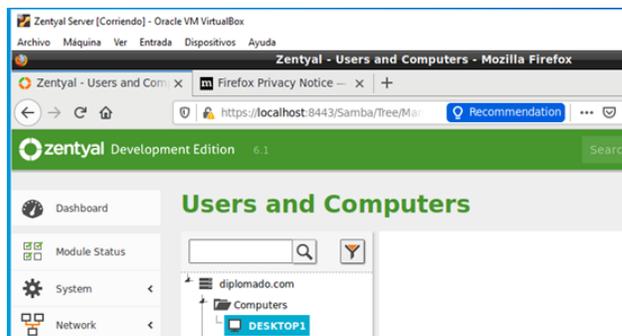


Fig. XXIX agregar el dominio

Nos logeamos con el usuario que hemos creado

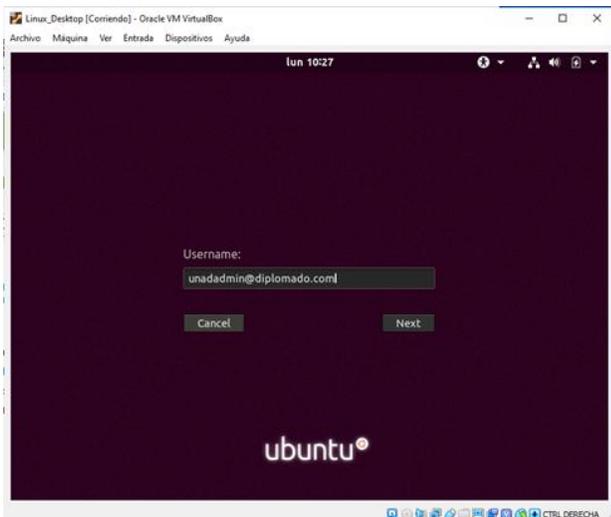


Fig. XXX inicio de sesión

De esta forma tenemos conectado nuestro Ubuntu desktop al dominio con Zentyal.

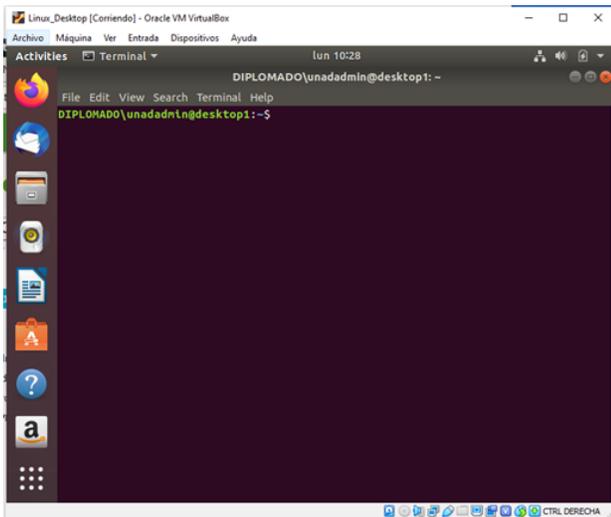


Fig. XXX conexión Ubuntu desktop y Zentyal

IV. SERVIDOR PROXY NO TRANSPARENTE

Un servidor proxy es un intermediario entre cliente y un servidor. La referencia a no transparente quiere decir visible para el usuario y cuya configuración se debe hacer en la máquina de este.

En esta sección se detalla la implementación bajo un ambiente gráfico Zentyal 6.0.

A. Requisitos

Tener instalado el servidor Zentyal en su versión 6.0 con dos interfaces de red: eth0 y eth1. A continuación se muestra los detalles de las interfaces:



Fig. XXXI Configuración de interface eth1.



Fig. XXXII Configuración de interface eth0.

Es importante destacar que la primera corresponde a la red interna virtualizada y la segunda es para la conexión dinámica hacia internet. Otro aspecto es la puerta de enlace, debiendo apuntar hacia la fuente de red del adaptador virtual. El módulo solicita un cortafuegos, el cual debe instalarse en la sección Gestión del software -> componentes de Zentyal.

B. Instalación de los módulos

Se requiere los módulos Cortafuegos y Proxy HTTP. Para hallarlos vamos a Gestión de Software -> Componentes de Zentyal

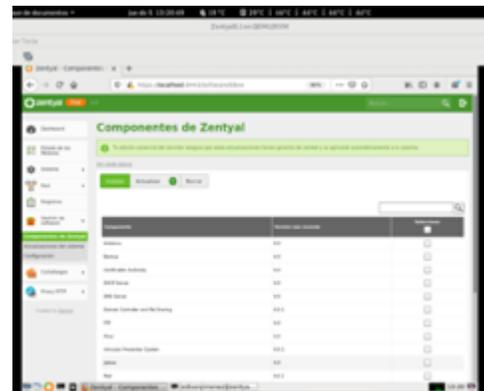


Fig. XXXIII Instalación complementos Zentyal

Para confirmar la instalación correcta solo basta con

observar el área izquierda inferior o ir a la sección estado de los módulos:



Fig. XXXIV configuración módulos

En caso de requerirse su activación inmediata se procede a marcar la casilla de estado.

C. Configuración de HTTP Proxy no transparente

Lo primero que se debe hacer es ingresar a las sección Red -> Objetos -> Añadir Nuevo. Una vez creado el objeto se debe crear los miembros en la sección respectiva del interfaz. En esta ingresamos todos los datos correspondientes a la máquina cliente, tal como se muestra en la siguiente figura:



Fig. XXXV añadir usuarios

El aspecto final de esta sección debe observarse como sigue:

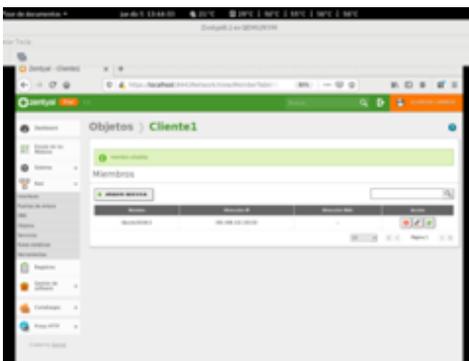


Fig. XXXVI cliente creado

Finalmente en la sección reglas de acceso se configura como Origen Objeto de Red a Cliente1 (Ubuntu18.04-2). La configuración debe quedar como denegar todo. A continuación se muestra la configuración final del módulo:

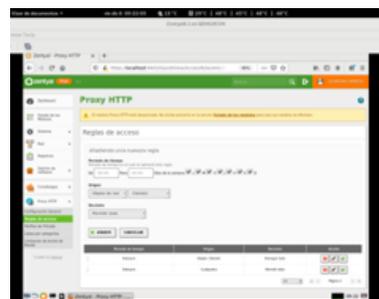


Fig. XXXVII origen de red

en esta característica fundamental.

D. Configuración en el cliente

Bueno, hasta aquí se ha realizado la configuración en la red. Para el cliente, basta con ingresar al navegador y dejar en preferencias una configuración como se muestra en la figura:

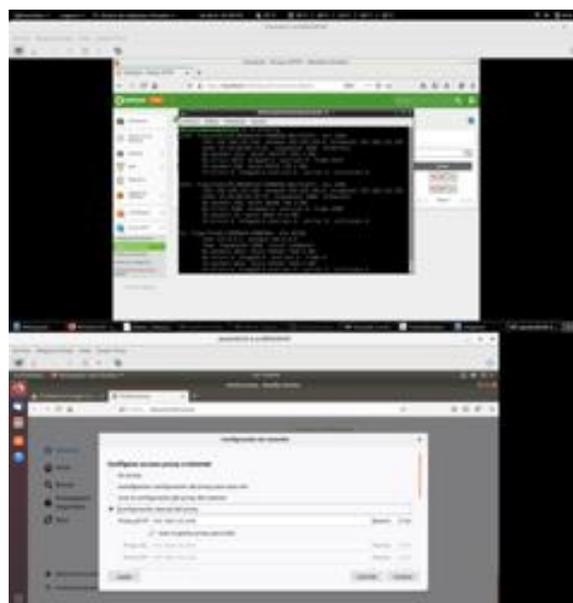


Fig. XXXVIII configuración de red

Se comprueba la conexión a la red virtualizada, por medio del icono superior derecha en la GUI del SO, pero aun así no permite conectarse a internet por medio del navegador:

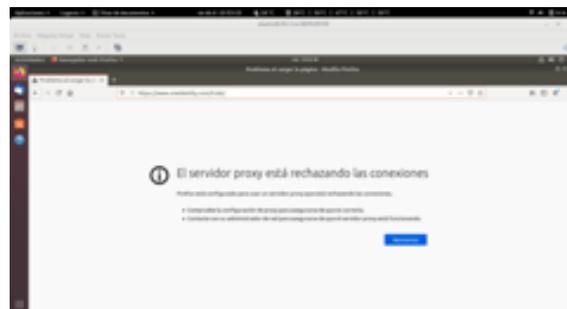


Fig. XXXIX servicio proxy

Introducción al Desarrollo de contenidos del tema.

Se inicia el proceso de instalación del sistema operativo PfSense, se acepta el acuerdo de licencia.

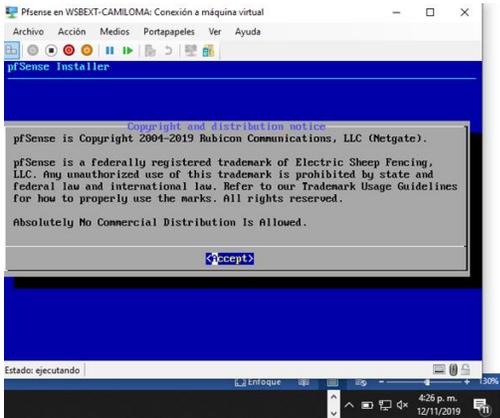


Fig. XL instalación PdSense

Se selecciona la opción "Install pfSense"

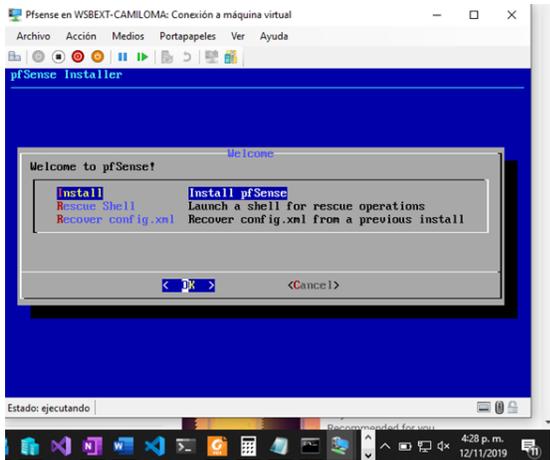


Fig. XLI instalación PdSense

Se selecciona la opción de teclado Latin America (accents Keys)

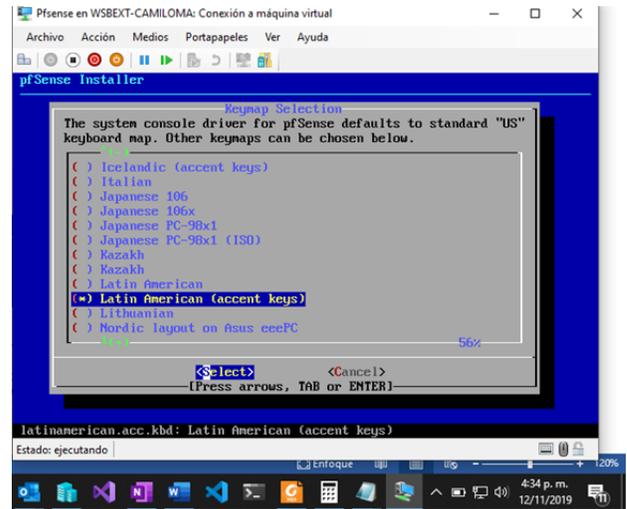


Fig. XLII instalación PdSense

Se selecciona la opción Auto(UFS) Guided Disk Setup

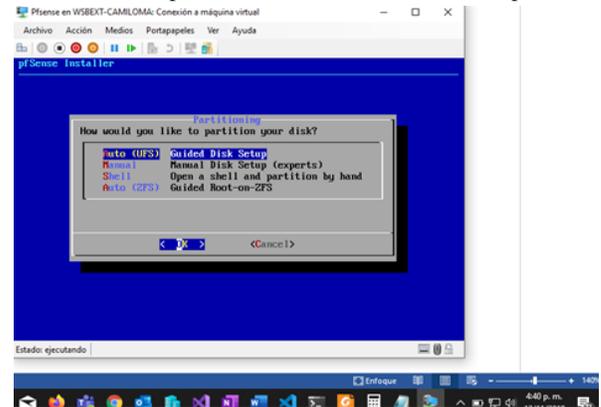


Fig. XLIII instalación PdSense

Inicia el proceso de particionado del disco e inicialización

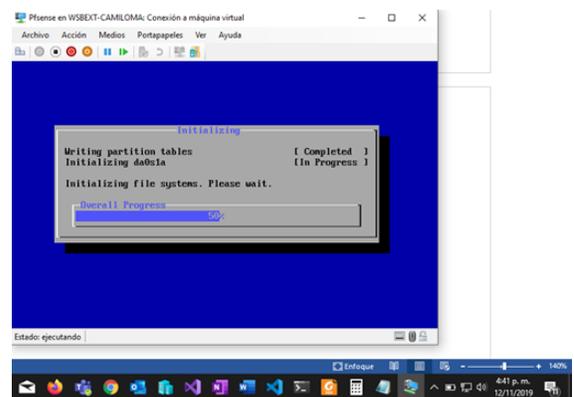


Fig. XLIV instalación PdSense

Extrayendo los archivos de la distribución.

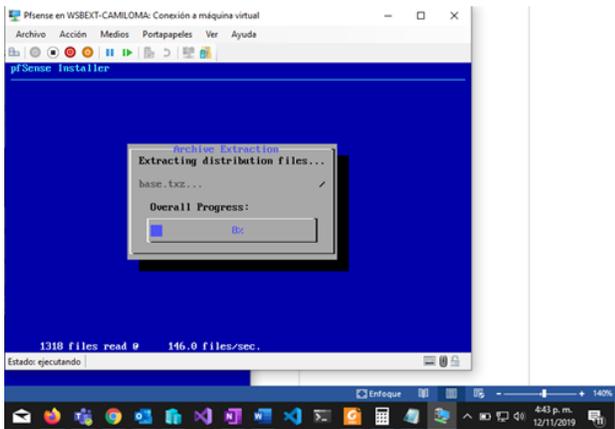


Fig. XLV instalación PdSense

Se indica que no se van a realizar modificaciones de manera manual.

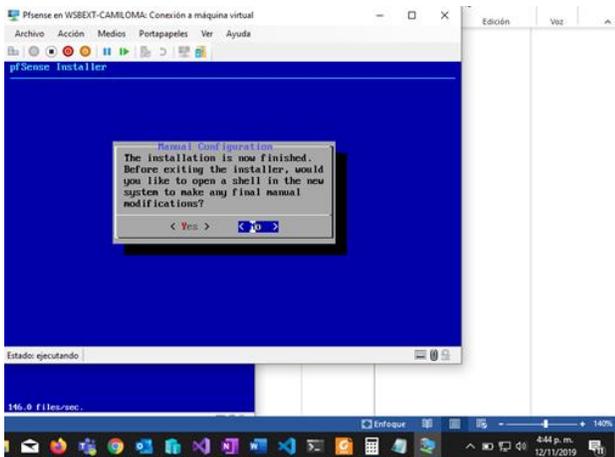


Fig. XLVI instalación PdSense

Finaliza la instalación de pfSense se selecciona la opción de reiniciar.

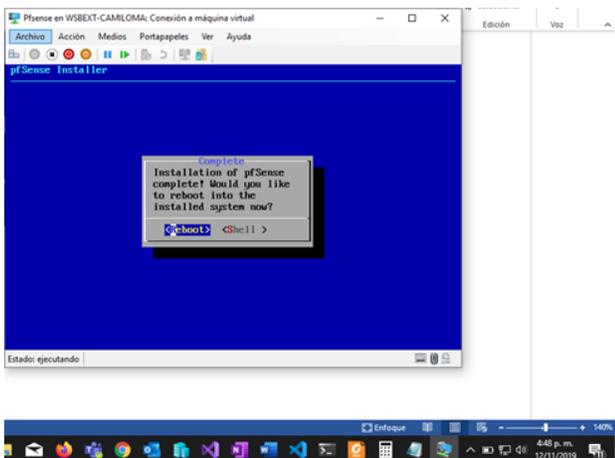


Fig. XLVII instalación PdSense

Se inicia el sistema, se indica que no se van a configurar las interfaces aun.

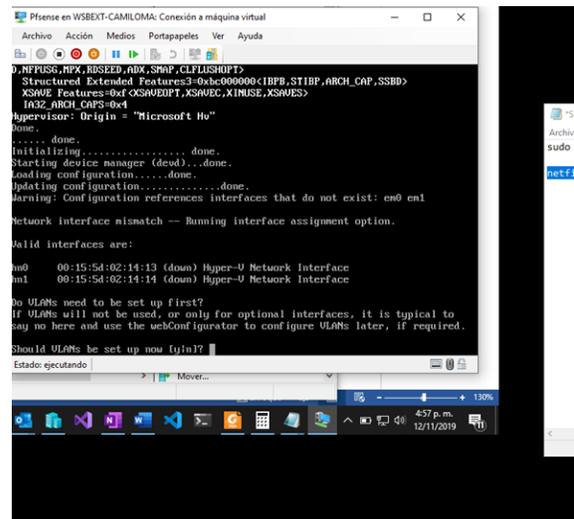


Fig. XLVIII configuración de interfaces de red

Se selecciona la interfaz WAN en este caso el conmutador virtual externo que proporciona acceso a internet.

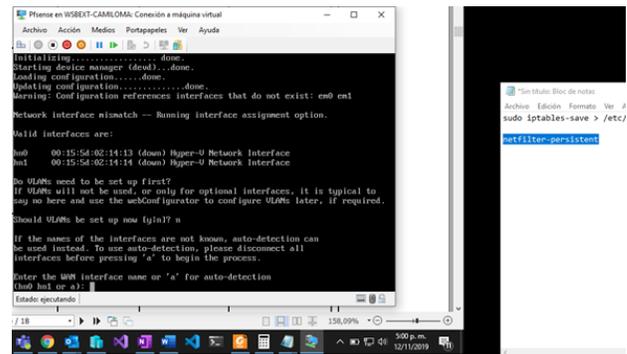


Fig. XLIX acceso a internet

Interfaz de red externa.

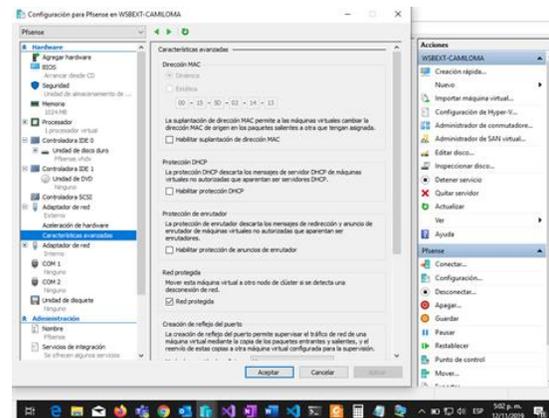


Fig. L configuración red externa

Se asigna la interfaz hn0 para la conexión WAN y la interfaz hn1 para la interfaz Lan.

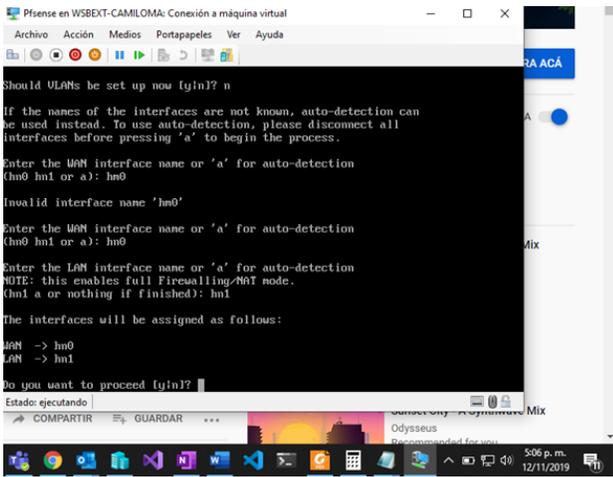


Fig. LII finalización de instalación

Ingresamos al panel de la administración con la IP interna 192.168.1.1

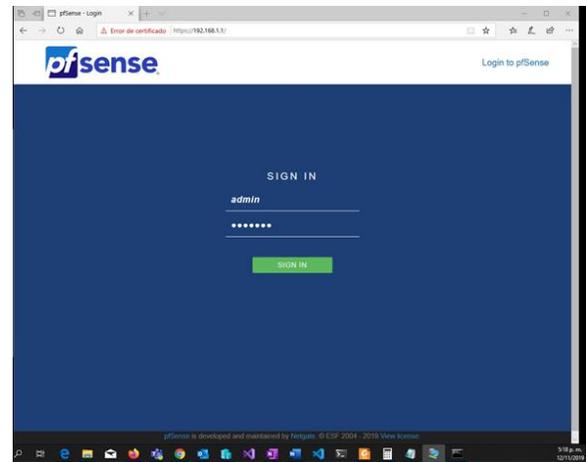
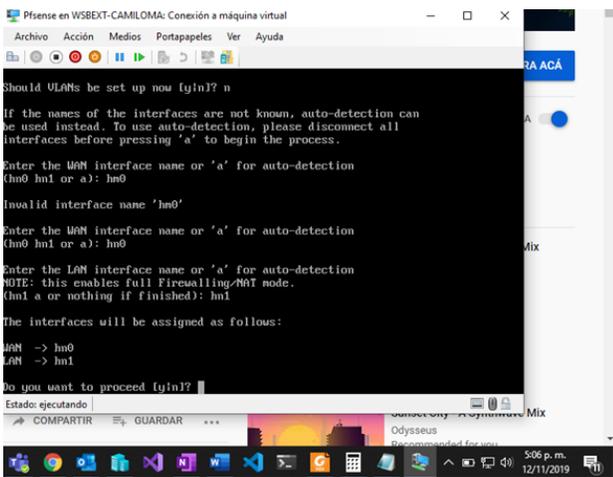


Fig. LIII ingreso sesión

Se visualiza el panel de inicio

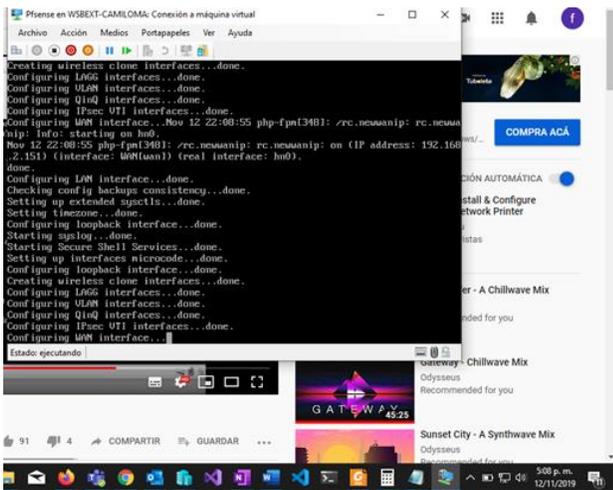


Fig. LI asignación de interfaces de red

Finaliza la instalación de pfsense.

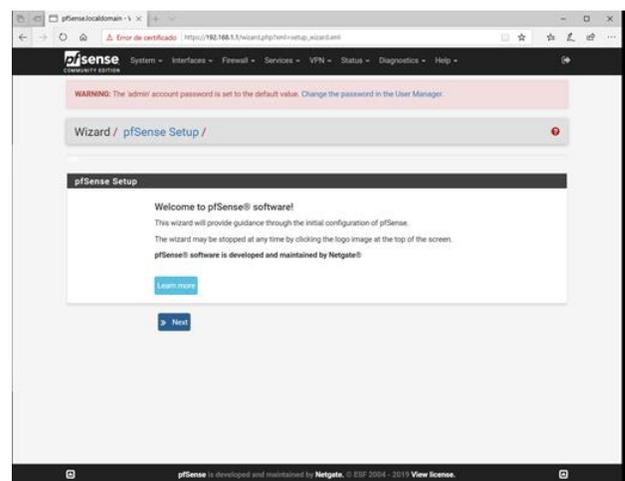


Fig. LIV panel de inicio

Se asigna el nombre del host

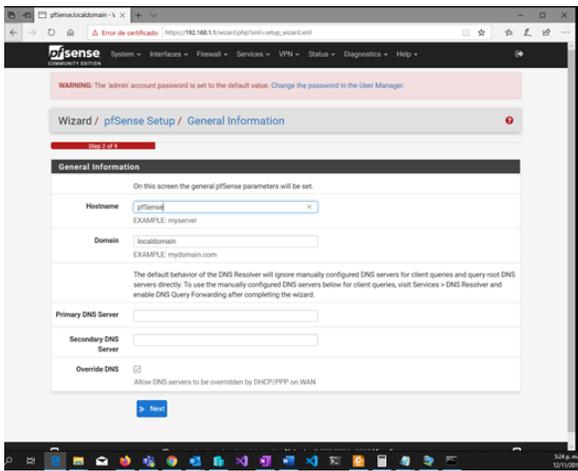


Fig. LV asignación host

Se establece el servidor de tiempo, y la zona horaria.

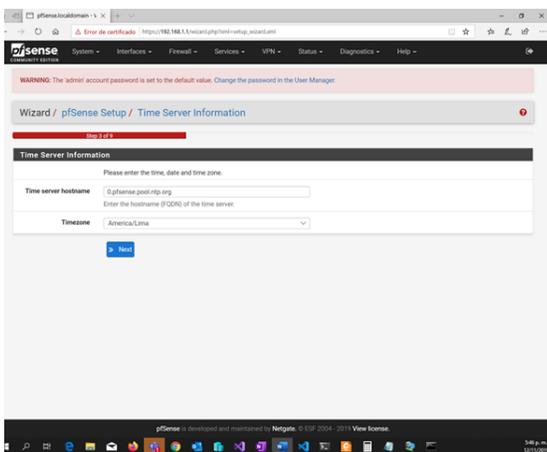


Fig. LVI establecer servidor

Se configura la interfaz LAN

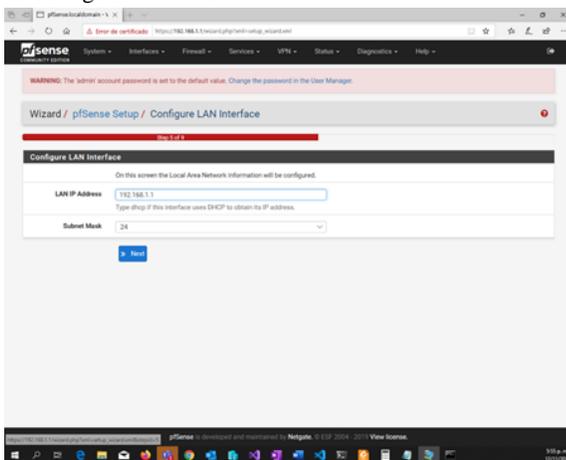


Fig. LVII configuración LAN

Se asigna la contraseña de administración de pfSense.

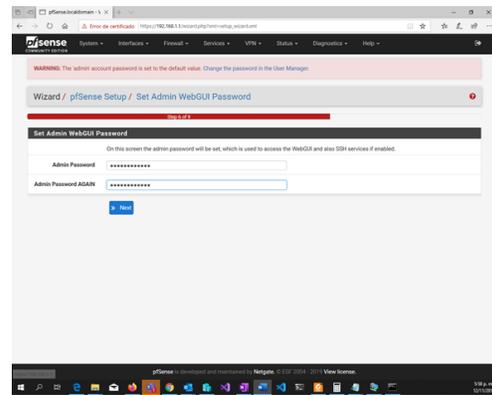


Fig. LVIII contraseña pfSense

Se carga la configuración

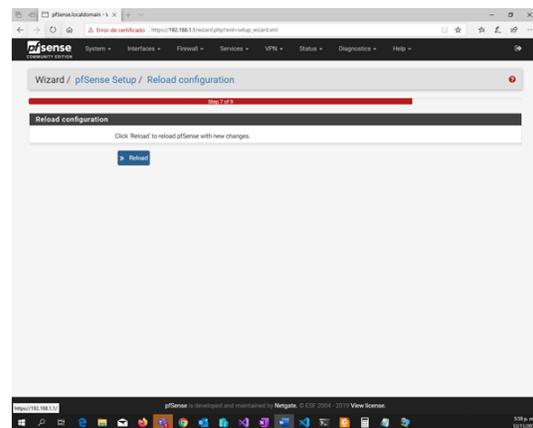


Fig. LIXI carga de configuración

Finaliza el proceso de configuración

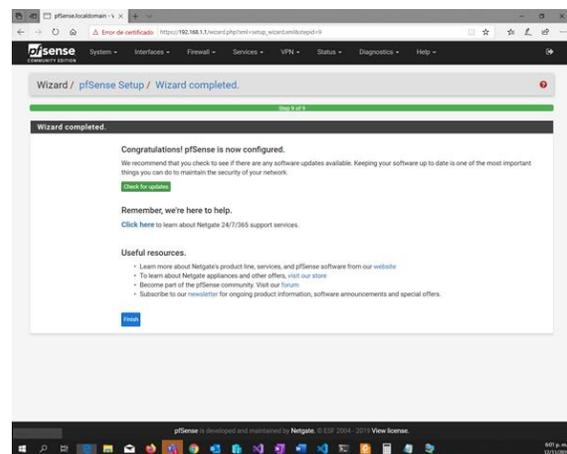


Fig. LX finalización configuración

Se visualiza el resumen de la configuración.

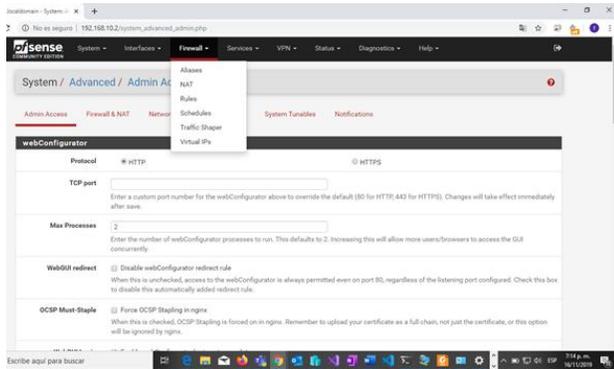


Fig. LXVIII Gestión tráfico

Interfaz que permite la gestión de servicios como Backup, portal cautivo, configuración DHCP, configuración DNS etc.

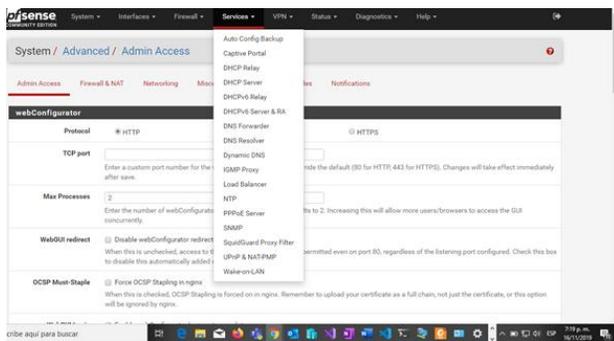


Fig. LXIX Gestión tráfico

Interfaz que permite la gestión de conexiones VPN.

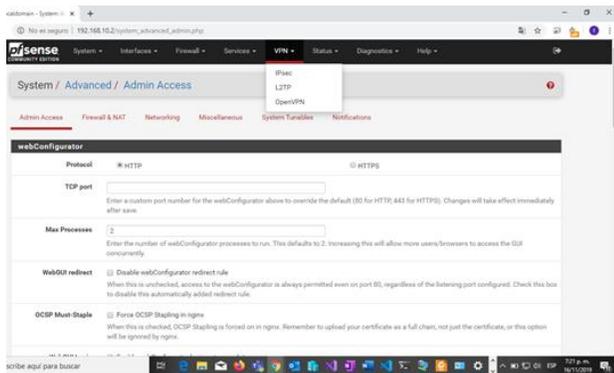


Fig. LXX Gestión VPN

Interfaz Estatus que permite identificar el estado de los servicios como portal cautivo, la asignación de direccionamiento por parte del servidor DHCP, los registros DNS, e interfaces de red etc.

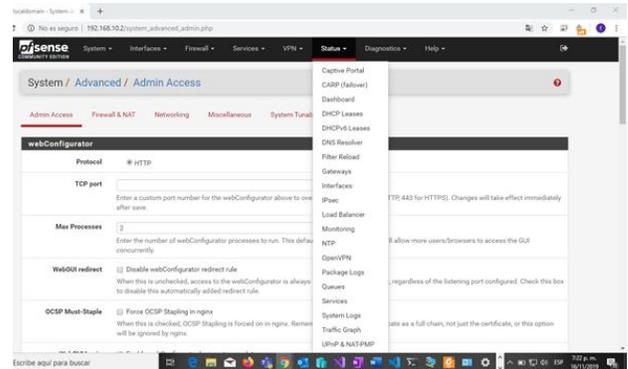


Fig. LXXI DNS

Interfaz de diagnósticos permite generar información de diagnóstico con respecto a los servicios provisionados dentro del firewall.

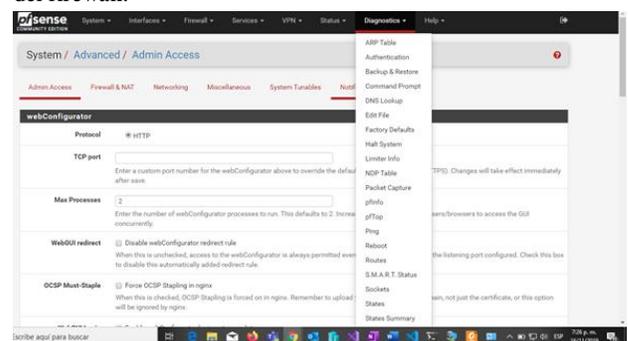


Fig. LXXII interface de diagnóstico

Interfaz ayuda, permite acceder a información correspondiente a la documentación del firewall Pfsense, y foro de usuarios.

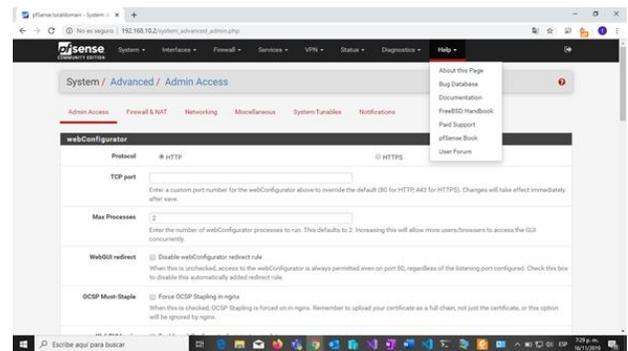


Fig. LXXIII interface de diagnóstico

Bloquear el Acceso a nuestro equipo desde la IP 192.168.1.10 a Tráves del puerto 22 en función del protocolo SSH. Se realiza Conexión SSH al servidor test.rebex.net



Fig. LXXIV bloqueo accesos

Se procede a generar la regla que bloquea la conexión al puerto 22 SSH

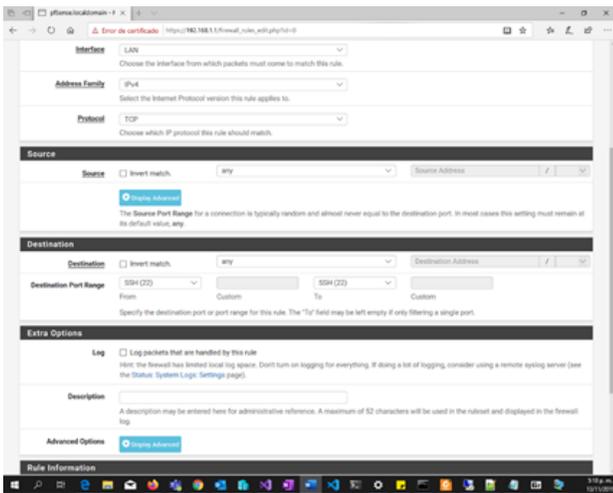


Fig. LXXV generación de regla

Se evidencia que no es posible realizar la conexión al servidor test.rebex.net



Fig. LXXVI evidencia de no conexión

Denegar el acceso a Internet para El Equipo con IP 192.168.1.10
Se identifica que el equipo con dirección IP 192.168.1.10 cuenta con conexión a internet

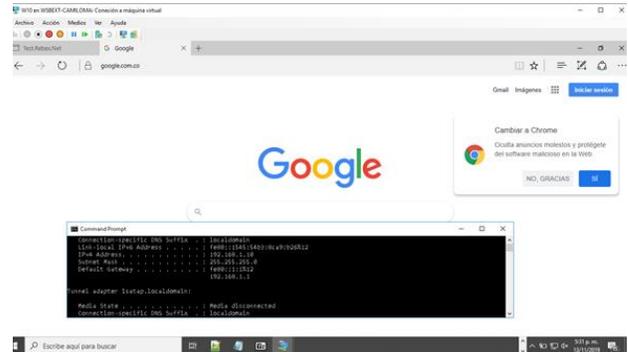


Fig. LXXVI denegación de acceso

Se genera la regla dentro del firewall para bloquear acceso a internet.

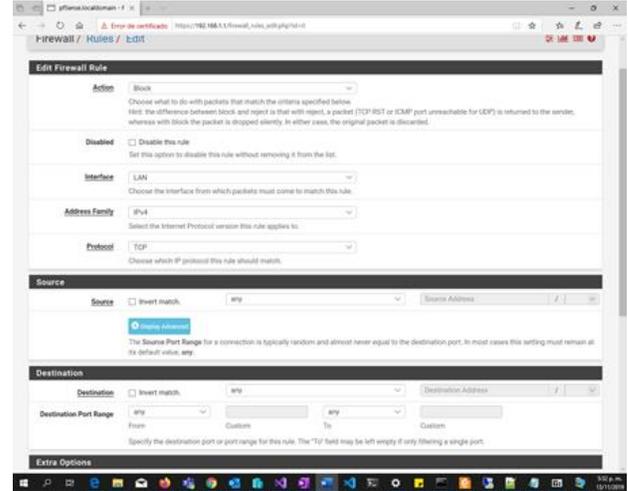


Fig. LXXVII regla de firewall

Se identifica que el equipo ya no cuenta con conexión a internet.

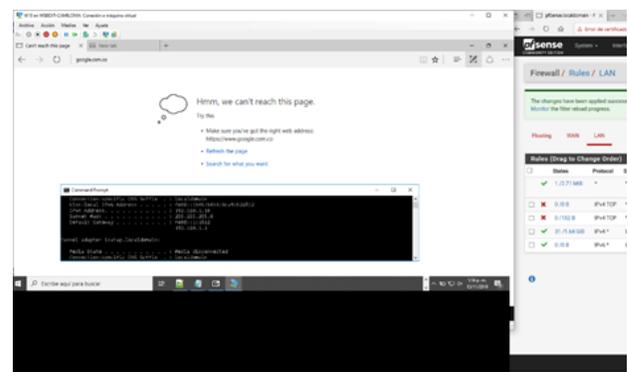


Fig. LXXVIII equipo sin conexión

Restringir el acceso a la aplicación Dropbox URL de descarga
Se identifica que la maquina con dirección IP 192.168.1.10 tiene acceso a la url de descarga de Dropbox.

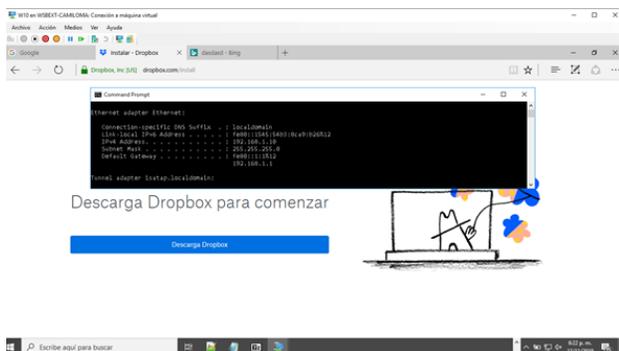


Fig. LXXIX restricción DROPBOX

Se genera la regla de firewall para que bloquee el acceso a la página de descarga de Dropbox.

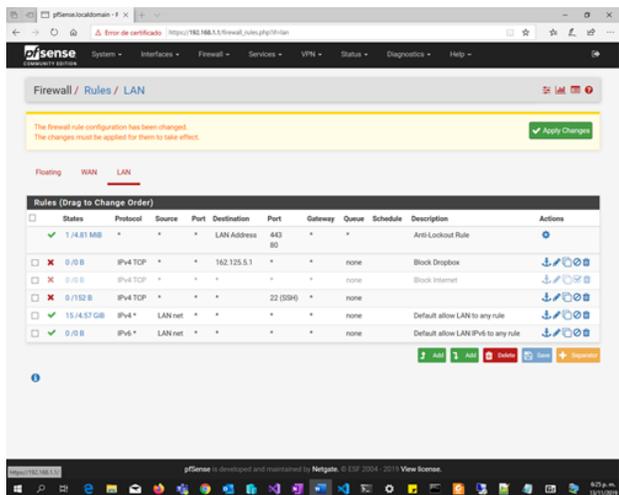
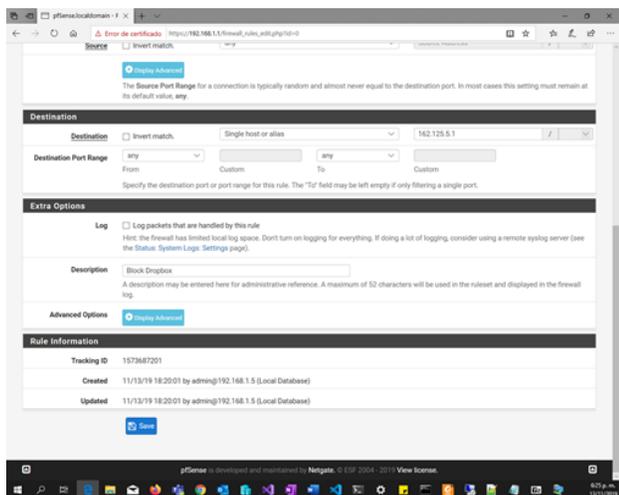


Fig. LXXIX restricción DROPBOX

Se identifica que yo se posee acceso a la página de Dropbox.com

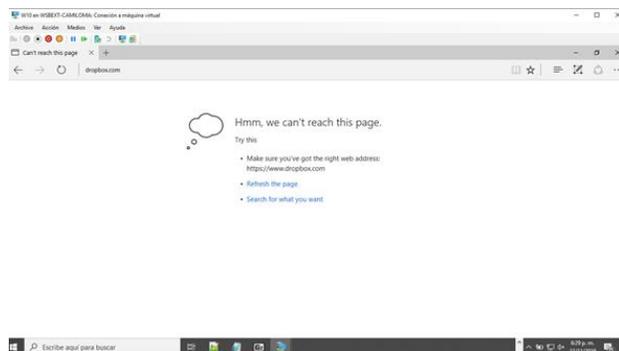


Fig. LXXX página sin acceso

VI. FILE SERVER y PRINT SERVER

se desarrolla los ítems del paso 8, en el cual se aborda los temas de configuración de servidor implementado LDAP,, mostrando las diferentes etapas de configuración desde la instalación del servidor, pasando por la configuración de los paquetes base y configurando los parámetros de LDAP, además se muestra la configuración del cliente de Ubuntu Para realizar la conexión con el servidor.

A. Instalacion y configuracion de los paquetes de ldap

En esta sección se selecciona el paquete necesario para instalar ldap con la dependencias de instalación de los otros paquetes como lo son dns, gestor de red y firewall

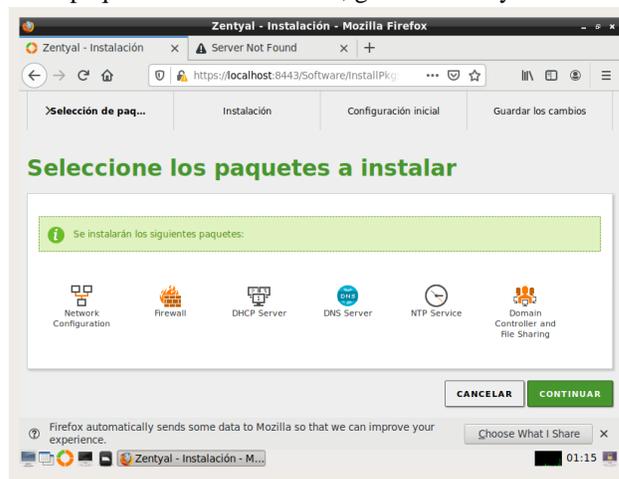


Fig. LXXX1 visualización de paquetes a instalar ldap

B. Configuración de interfaces de red

En esta sección se configura las tarjeta de red que serán administradas por el sistemas y servirán de puente de comunicación entre las diferentes máquinas

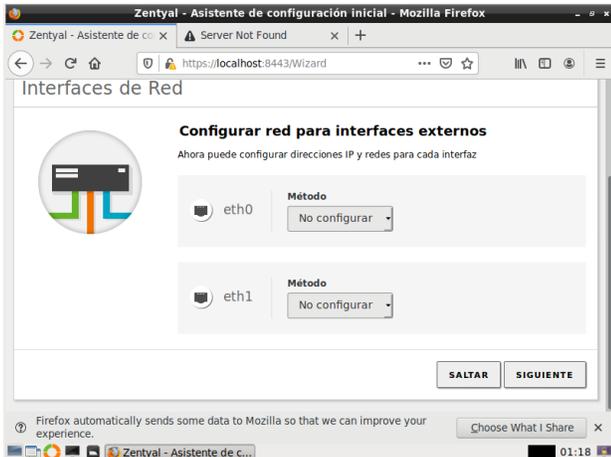


Fig. LXXXII Selección de interfaces de red

C. Configuración inicial del servidor de dominio

En esta sección se configura el nombre del dominio el cual será implementado por las máquinas clientes

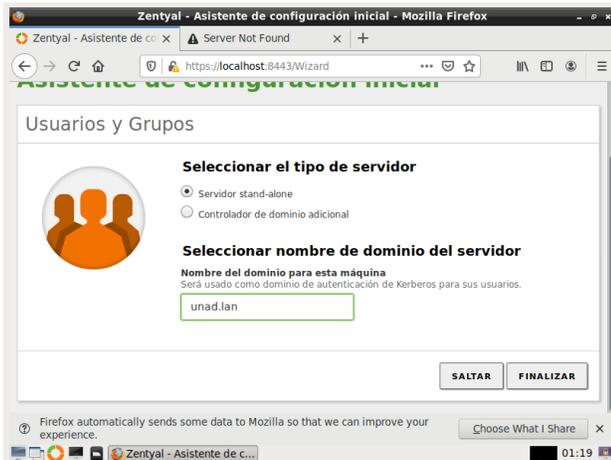


Fig. LXXXIII Configuración inicial de LDAP

D. Visualización de mensaje de aplicar los cambios

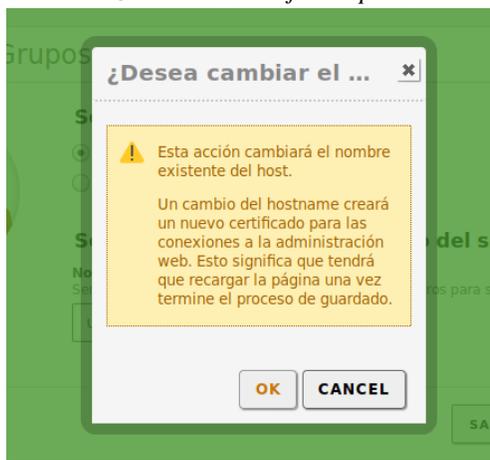


Fig. LXXXIV Mensaje de aplicar los cambios

E. Visualización de mensaje de finalización

Se visualiza el mensaje, en este punto ya se encuentra el servidor listo para su funcionamiento, el cual proporciona un dashboard para su interacción

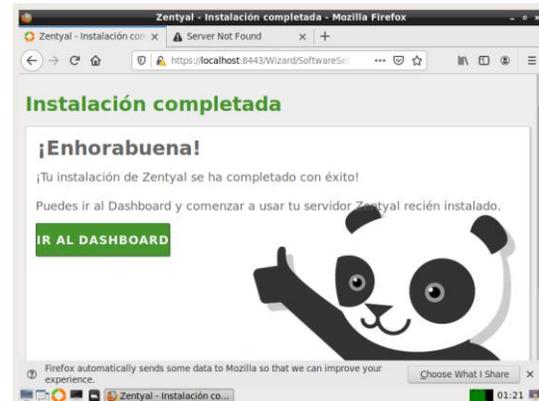


Fig. LXXXV mensaje de finalización de la instalación

F. Visualización del dashboard

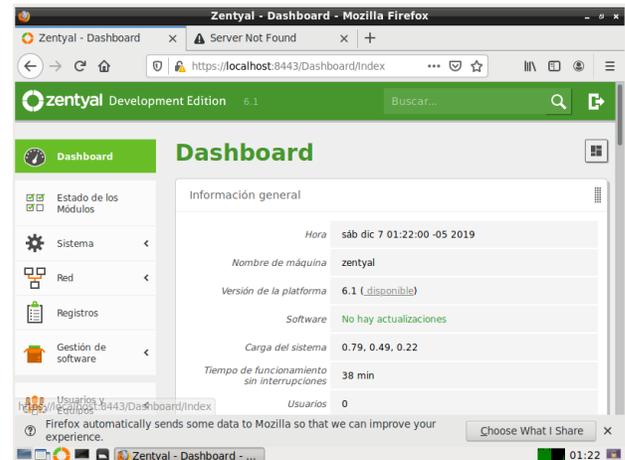


Fig. LXXXVI interfaz del dashboard

G. Visualización de la configuración del dominio

En esta sección se configura para que las conexiones sean móviles esto permite que un usuario pueda autenticarse en diferentes terminales

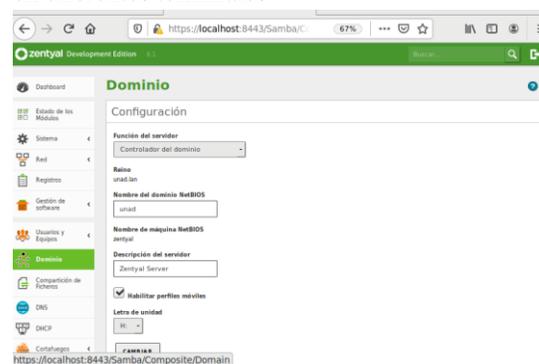


Fig. LXXXVII configuración móvil del dominio

H. Visualización de la configuración del dominio

En esta sección se puede identificar los equipos

conectados al servidor de LDAP así como lo clientes que pueden autenticarse en las terminales

En esta sección se visualiza la instalación de paquetes para la configuración al servidor de LDAP

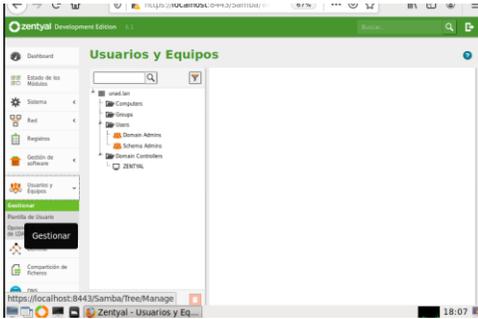


Fig. LXXXVIII Interfaz de administración de usuarios y equipos

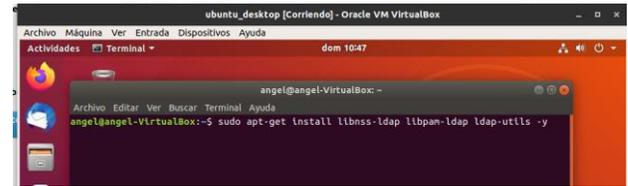


Fig. XCI Instalación de paquetes para la comunicación - LDAP

I. Creación de un usuario

En esta sección se visualiza la creación de un usuario en el sistema, este se puede definir que sea en un grupo administrador o no pertenecer a ningún grupo

L. Interfaz para la conexión con el servidor de LDAP
Se ingresa la IP del servidor

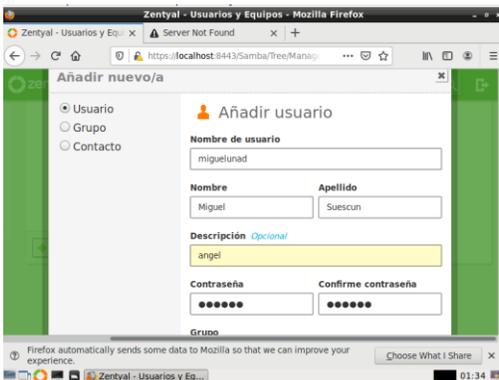


Fig. LXXXIX Interfaz de creación de usuario

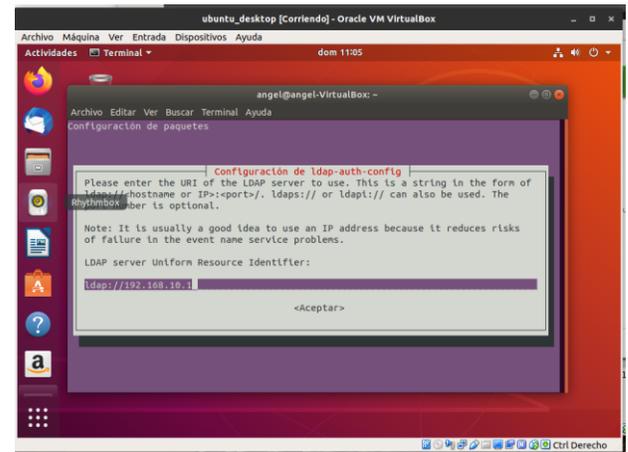


Fig. XCII Configuración de conexión con el servidor

J. Configuración global de LDAP

En esta sección se visualiza los datos para realizar la conexión al servidor de LDAP

M. Configuración de acceso al servidor
En esta sección se ingresa el dominio y de la conexión con el servidor de LDAP

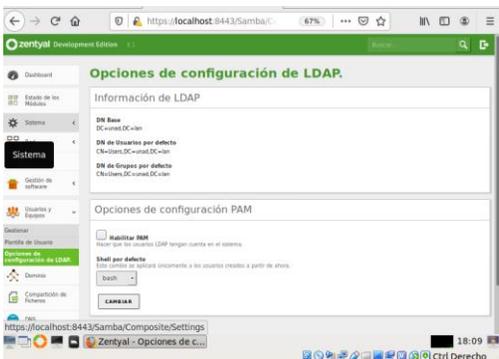


Fig. XC Interfaz de información de LDAP

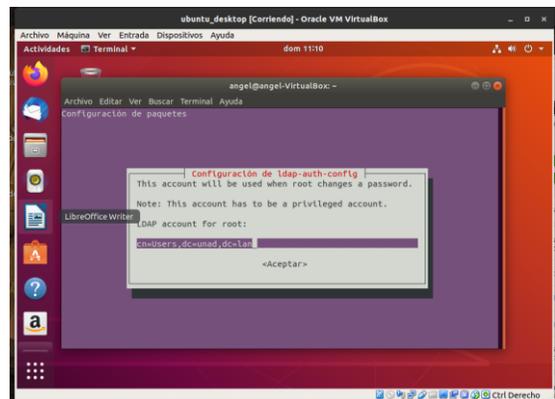


Fig. XCIII Configuración de acceso por dominio

K. Configuración de cliente Ubuntu - Instalación de dependencias

VII. VPN

Una red privada virtual (RPV), en inglés: Virtual Private Network (VPN), es una tecnología de red de ordenadores que permite una extensión segura de la red de área local (LAN) sobre una red pública o no controlada como Internet.

Para el ejercicio a realizar en Zentyal, se implementara una VPN con OpenVPN que favorece su funcionamiento en distribuciones Linux

A. instalación paquetes para el funcionamiento de la VPN

Para el funcionamiento de la VPN, debemos instalar en la máquina los paquetes de Network configuration, Firewall, Certification Authority y VPN

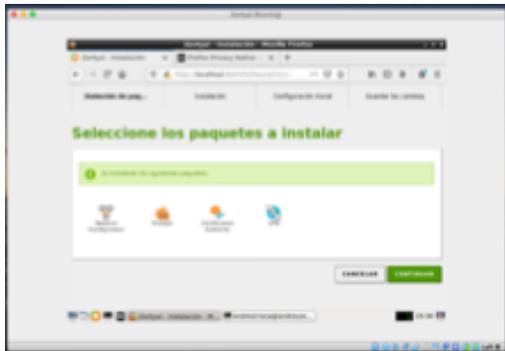


Fig. XCIV Instalación paquetes VPN

En este proceso se configuran las interfaces de red indicadas al inicio en el momento que configuración de la máquina virtual

B. Creación certificado de autoridad

Se deben crear los certificados de autoridad para el funcionamiento de la VPN a crear, en este creamos el nombre, código del país, Ciudad, Estado y Días de expiración.

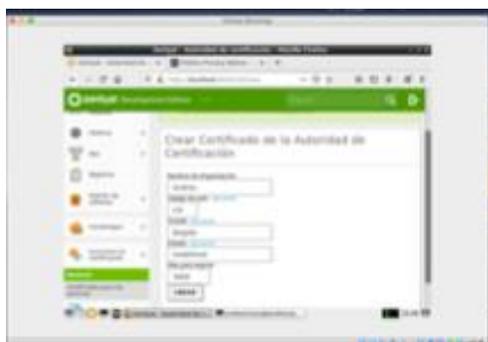


Fig. XCV Certificación de autoridad

C. Creación servicios de VPN

Se crean los servidores de VPN a utilizar, para este ejemplo, se configura andrest.vpn, que será el servidor a usar en esta implementación .



Fig. XCVI Servidores VPN

D. Creación del certificado del servidor

Para el funcionamiento de la VPN, es necesario instalar un certificado el cual para este ejercicio se denomina certificado-servidor

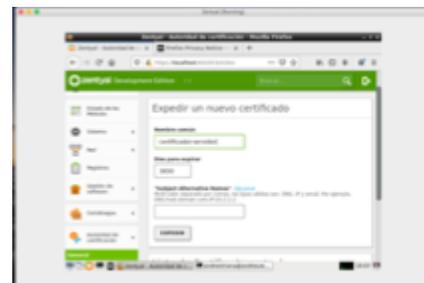


Fig. XCVII Certificados del servidor

E. Configuración VPN del servidor

En este proceso, se configura el puerto, la dirección IP, el certificado del servidor



Fig. XCVIII configuración VPN del servidor

F. Configuración de servicios

Se crean los servicios a usar para la VPN

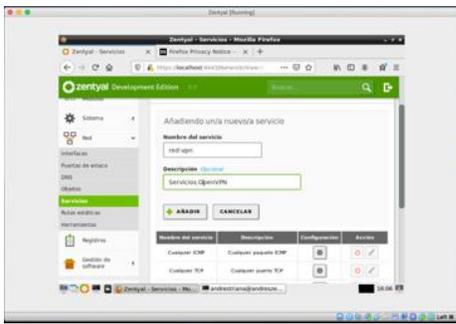


Fig. XCIX configuración de servicios



Fig. CII Descarga de los paquetes

G. Instalación puerto único

En el caso de que nuestra VPN utilice el protocolo de código abierto OpenVPN, el puerto que necesitamos será el número 1194 UDP



Fig. C configuración puerto único

H. Configuración cortafuegos (firewall)

Se configura el firewall, para garantizar la seguridad de la VPN que se está implementando, añadiendo las reglas identificadas

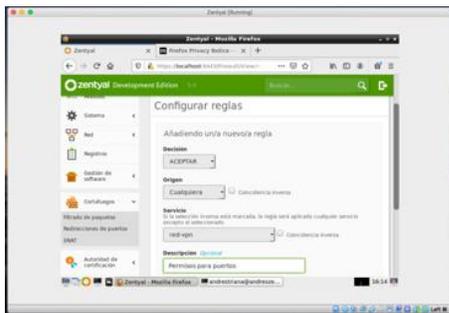


Fig. CI configuración cortafuegos

I. Descargar paquetes de configuración

De acuerdo a donde se va a implementar la VPN, se descarga la configuración para Linux o Windows, en este caso es el primero

J. Instalación OpenVPN en cliente y funcionamiento

En el desktop Ubuntu cliente, se instala OpenVPN con el comando apt-get install Openvpn



Fig. CIII instalación OpenVPN en cliente

Se configura el cliente ubicándonos en la carpeta de descarga de la configuración y se ejecuta el comando sudo openvpn --config andrest.vpn-client.conf

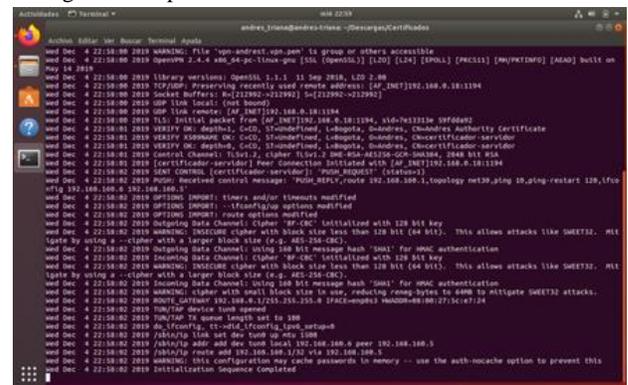


Fig. CIV configuración OpenVPN en cliente

Se comprueba en el cliente por medio de un ifconfig, que la instalación de la VPN se realizará, asignada a la dirección 192.168.160.6

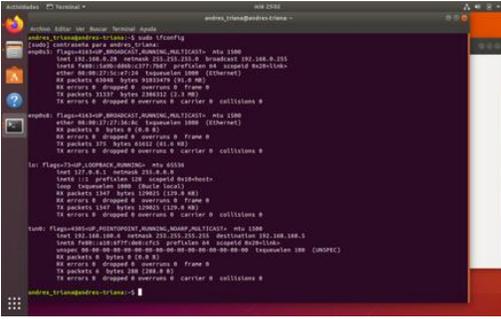


Fig. CV verificación instalación VPN

VII. CONCLUSIONES

Contar con herramientas gráficas, lo tradicional en windows, puede suponer una ventaja inicial para la configuración de distintos servicios en linux; sin embargo, la dependencia alta de las versiones a programas y librerías específicas puede llegar a ser un verdadero dolor de cabeza para el administrador. Con lo anterior se suma que, toda herramienta gráfica, normalmente trae un costo asociado, por lo que la ventaja competitiva de GNU/Linux como alternativa a Windows Server se ve limitada y puede llegar a quedar sin fundamento

Como conclusión vemos que Zentyal, se desarrolló con el objetivo de acercar Linux a las pymes y permitirles aprovechar todo su potencial como servidor de empresa. Es la alternativa en código abierto a los productos de Microsoft para infraestructura TIC en las pymes (Windows Small Business Server, Windows Server, Microsoft Exchange, Microsoft Forefront...) y está basado en la popular distribución Ubuntu. Zentyal permite a profesionales TIC administrar todos los servicios de una red informática, tales como el acceso a Internet, la seguridad de la red, la compartición de recursos, la infraestructura de la red o las comunicaciones, de forma sencilla y a través de una única plataforma.

RECONOCIMIENTOS

Reconocimiento especial a la institución por la formación realizada para poder implementar y desarrollar el artículo, dando las capacidades y conocimientos necesarios en función de lo solicitado

Por otra parte, a todos nuestros familiares por el apoyo emocional y económico a lo largo de la carrera, que gracias a ellos podemos finalizar con éxito los requerimientos para ser excelentes profesionales .

REFERENCIAS

- [1] S. M. Metev and V. P. Veiko, Laser Assisted Microtechnology,
- [9] "PDCA12-70 data sheet," Opto Speed SA, Mezzovico, Switzerland.

Es.wikipedia.org. (2019). Zentyal. [online] Available at: <https://es.wikipedia.org/wiki/Zentyal> [Accessed 5 Dec. 2019].