MIGRACION DEL SERVICIO DE AUTENTICACION DEL DIRECTORIO ACTIVO DE WINDOWS A LA PLATAFORMA DE SOFTWARE LIBRE EBOX EN VITELSA S.A

PAULA ANDREA SANCHEZ LUNA

UNIVERSIDAD INDUSTRIAL DE SANTANDER

FACULTAD DE INGENIERIAS FISICO MECANICAS

ESCUELA DE INGENIERIA ELECTRICA, ELECTRONICA Y TELECOMUNICACIONES

BUCARAMANGA

2011

MIGRACION DEL SERVICIO DE AUTENTICACION DEL DIRECTORIO ACTIVO DE WINDOWS A LA PLATAFORMA DE SOFTWARE LIBRE EBOX EN VITELSA S.A

PAULA ANDREA SANCHEZ LUNA

Monografía presentada como requisito para optar al título de Especialista en Telecomunicaciones

Director:

ING. JORGE HERNANDO RAMON SUAREZ

UNIVERSIDAD INDUSTRIAL DE SANTANDER

FACULTAD DE INGENIERIAS FISICO MECANICAS

ESCUELA DE INGENIERIA ELECTRICA, ELECTRONICA Y TELECOMUNICACIONES

BUCARAMANGA - 2011

TABLA DE CONTENIDO

LISTA DE FIGURAS

LISTA DE TABLAS

RESUMEN

TITULO

MIGRACION DEL SERVICIO DE AUTENTICACION DEL DIRECTORIO ACTIVO DE WINDOWS A LA PLATAFORMA DE SOFTWARE LIBRE EBOX EN VITELSA S.A*

AUTOR: Paula Andrea Sanchez Luna**

PALABRAS CLAVES

Software Libre, Gestión de redes para PYMES, Distribución Ubuntu Server Edition, Directorio Activo, Balanceo de Cargas-Ancho de Banda, Autoadministrable.

DESCRIPCION

Este trabajo presenta una descripción somera de la plataforma de software libre ZENTYAL PLATFORM. Se quiso mostrar sus principales funcionalidades haciendo énfasis en la sencillez de su administración y configuración. La finalidad del proyecto aquí planteado consiste en mostrar al especialista encargado de administrar redes en las pequeñas y medianas empresas una opción libre de costos de licenciamiento administrable desde un entorno web sin las limitantes de requerir amplios conocimientos en un entorno Linux y totalmente capaz de manejar los requerimientos dentro de las organizaciones así como lo hace un Sistema Windows Server.

Para la organización tomada como modelo VIDRIOS TEMPLADOS Y LAMINADOS DE SANTANDER- VITELSA S.A queda el beneficio de mejorar la administración de su red interna, donde además de mejorar sus políticas de seguridad han ganado una disminución de costos en el licenciamiento del software y están cumpliendo con las políticas de licenciamiento de software acorde a la Ley 603 de 2000 emitida por el Congreso Colombiano. Migrar el directorio activo de esta organización de su sistema antiguo Windows server hacia Zentyal fue una tarea sencilla de realizar y cumplió con el objetivo principal del proyecto, además la operación dentro de la organización garantizo una satisfacción en las directivas en cuanto a el mejoramiento de su seguridad.

---

* Monografía de Grado

**Facultad de Ingeniería Físico-Mecánicas, Escuela de Ingeniería Eléctrica, Electrónica y Telecomunicaciones, Programa de Especialización en Telecomunicaciones, Director del Proyecto: Ingeniero Jorge Hernando Ramón Suarez

ABSTRACT

TITLE:

MIGRATION OF THE SERVICE AUTHENTICATION OF WINDOWS ACTIVE DIRECTORY TO THE SOFTWARE FRE EBOX PLATFORM IN VITELSA S.A *

AUTHOR: Paula Andrea Sanchez Luna**

KEY WORDS

Free Software, Network Management for PYMES, Distribution Ubuntu Server Edition, Active Directory, Load Balancing-Bandwidth, self-administered

DESCRIPTION:

This paper presents a brief description of the software free for download ZENTYAL PLATFORM. Wanted to show its main features emphasizing in the simplicity of it administration and configuration. The purpose of the project proposed here is to show the specialist responsible for managing networks in small and medium-sized businesses an option free of licensing costs, manageable from a web environment without the limitations of require extensive knowledge in a Linux environment and fully capable of handling the requirements within the organization as well as Windows Server System does.

For the organization taken as a model VIDRIOS TEMPLADOS Y LAMINADOS DE SANTANDER - VITELSA SA is the benefit of improving management of your internal network, where in addition to improving their security policies have won reduced costs in software licensing and are serving with software licensing policies according to the law 603 of 2000 issued by the Colombian Congress. The migration of the Active Directory in this organization of its Windows server old system to the new Zentyal platform was a task easy to perform and comply with the objective of the project. In addition the operation within the organization guarantees a satisfaction in the management about safety improving.

* Grade Monograph

** Physical-Mechanical Enginnering Division, School of Electric, Electronic and Telecommunications Enginnering, Specialization Program in Telecommunications, Manager: Engineer Jorge Hernando Ramon Suarez

INTRODUCCION

La tendencia de las organizaciones está orientada hacia redes grandes y complejas que soportan muchos usuarios y aplicaciones. El gestionar estas redes requiere de una inversión significativa en compra de software que permita administrar de manera eficiente los recursos y servicios que demandan la operación dentro de una organización.

Dentro de la región es muy frecuente encontrar organizaciones que han tenido que pagar altos costes por Licencias de Software para sus servidores y adicionalmente cargar costes por los permisos de los usuarios para el uso del software. Puntualmente hablando de un sistema para un servidor que opere bajo Windows, se requiere de la licencia del sistema operativo para el servidor y adicional se debe pagar por los accesos de los clientes al mismo.

EBOX Platform se presenta como una opción de servidor de código abierto para las pequeñas y medianas empresas funciona sobre el sistema operativo GNU/Linux con la distribución Ubuntu Server Edition y permite gestionar muchos servicios tales como: PDC (Controlador de Dominio Primario), VPN (Redes Privadas Virtuales), DHCP (Dynamic Host Configuration Protocol), Proxy, Correo, Firewall y muchos otros más servicios. Por tal motivo la migración a plataformas como EBox, se convierte para las organizaciones en una ventaja competitiva debido a la reducción de costes en inversión de software.

Durante el desarrollo de esta monografía EBox Platform cambio su nombre a ZENTYAL (Inicio desde Septiembre 01 de 2010). La descarga oficial de este sistema puede hacerse desde su página principal de internet: http://www.zentyal.com/es/products/ .

1 JUSTIFICACION

Los altos costos que tiene que pagar una empresa por licenciamiento de software en sus servidores se pueden mitigar con el uso de Herramientas de Software libre que sean robustas. Para este proyecto se ha tomado como modelo a la Organización VITELSA S.A, organización que cuenta con cerca de 120 usuarios actualmente y próximamente crecerá en cerca de 30 usuarios más debido a la creación de una nueva planta dentro de la región.

Esta empresa tiene instalado en sus servidores Sistemas Windows pero por su crecimiento requiere invertir los recursos en su infraestructura de producción y disminuir los costos que trae consigo la adquisición de software.

Es por ello que este trabajo beneficiara tanto a la organización VITELSA S.A como a los estudiantes que consulten este proyecto cuyo propósito es dar una guía básica de instalación, configuración y migración de un sistema Windows a un sistema sobre EBOX Platform.

Adicionalmente, este trabajo de grado me permite aplicar los conocimientos recibidos en la Especialización de Telecomunicaciones de la Universidad Industrial de Santander.

2 GLOSARIO

Network Time Protocol (NTP): Fue diseñado para sincronizar los relojes de las computadoras sobre una red no fiable, con latencia variable. Este servicio escucha en el puerto 123 del protocolo UDP. Está diseñado para resistir los efectos de la latencia variable (*jitter*).

Latencia: se denomina latencia a la suma de retardos temporales dentro de una red Un retardo es producido por la demora en la propagación y transmisión de paquetes dentro de la red.

Jitter: la diferencia entre el tiempo en que llega un paquete y el tiempo que se cree que llegara el paquete.

DHCP: (*Dynamic Host Configuration Protocol*) es un protocolo que permite a un dispositivo pedir y obtener una dirección IP desde un servidor que tiene una lista de direcciones disponibles para asignar

PAE/NX: En informática, extensión de dirección física (en inglés, Physical Address Extension o PAE) se refiere a una característica de los procesadores x86 que permite a los sistemas de 32-bit utilizar hasta 64 gigabytes (64 GiB) de memoria física, suponiendo que el sistema operativo proporcione el adecuado soporte. PAE está disponible en las CPUs Intel Pentium Pro y superiores (incluyendo todos los procesadores de la serie Pentium posteriores excepto las versiones con bus de 400 MHz del Pentium M), además de ciertos procesadores compatibles como los de AMD. Las aplicaciones software que necesitan acceso a más de 4 GiB de memoria el sistema operativo puede ofrecer algún mecanismo especial además del soporte PAE básico

Squid: Es un proxy cache Web para el apoyo de HTTP, HTTPS, FTP. Reduce los

tiempos de respuesta y mejora el ancho de banda mediante el almacenamiento en caché de las páginas más frecuentemente solicitadas.

OSPF: Protocolo de enrutamiento. Mantiene la topología de red completa y determina la ruta más corta a cada destino. Se envían solo los cambios que ocurren en la topología y no la tabla completa.

RIP: Es un protocolo de enrutamiento llamado vector distancia. En este algoritmo la tabla de enrutamiento es pasada completamente a los routers vecinos. De modo que cada router mantiene las tablas de enrutamiento de sus vecinos. Este proceso de envió se hace de forma periódica.

3 OBJETIVOS

3.1 OBJETIVO GENERAL

Realizar la migración del servicio de autenticación del directorio activo de Windows a EBOX Platform en la empresa Vitelsa S.A sede de Bucaramanga.

3.2 OBJETIVOS ESPECIFICOS

- Documentar las principales funcionalidades de EBOX Platform.
- Elaborar un manual de instalación y configuración EBOX Platform ajustado a la operación de VITELSA S.A
- Migrar el directorio activo de Windows a EBOX Platform haciendo uso del servicio de directorio LDAP.

4 QUE ES EBOX PLATFORM (ZENTYAL)

Es un software que funciona sobre el sistema operativo GNU/Linux con la distribución Ubuntu Server Edition. Puede ser instalado sobre una maquina virtual o sobre un recurso hardware físico (servidor). Esta plataforma de gestión ayuda a manejar y administrar de manera eficiente los servicios que se encuentran en las redes de tamaños medianos y pequeños (redes de PYMES), tiene una licencia libre (GPL)[5] y puede ser descargado de internet. Puede considerarse como el paralelo en software libre a la versión Small Business Server de Windows con una reducción de costos en un 100%.

Su administración se hace a través de una interfaz web bastante sencilla y en general está dividido en cinco módulos que ofrecen cada uno diferentes servicios. Estos Módulos son los siguientes:

1. GATEWAY
2. UTM (Unified Threat Manager)
3. INFRAESTRUCTURE
4. OFFICE
5. UNIFIED COMUNICATIONS

Toda la configuración de cada uno de los estos servicios es escrita por eBox de manera automática, para ello utiliza un sistema de plantillas. Con esta automatización se evitan los posibles errores cometidos de forma manual y ahorra a los administradores el tener que conocer los detalles de cada uno de los formatos de los ficheros de configuración de cada servicio (para quienes no son muy expertos en configuraciones Linux). Por tanto, no se requiere editar los ficheros de configuración originales del sistema ya que se sobrescribirán al guardar cambios debido a la gestión automática de eBox. Esta forma de operación minimiza la curva de aprendizaje para los administradores, representa un ahorro

[5] **GPL** (GNU General Public License): Licencia de software que permite la libertad de redistribución, adaptación, uso y creación de obras derivadas con la misma licencia.

de tiempo y minimiza los riesgos por una mala configuración en los archivos del sistema.

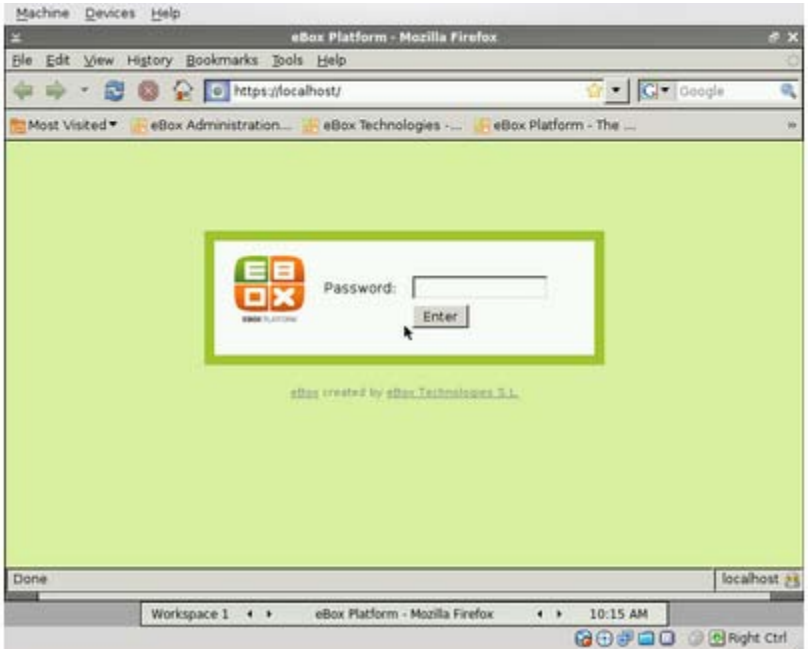


Figura 1. Interfaz Web de Administración EBox

4.1 DESCRIPCION DE LOS MODULOS QUE FORMAN EBOX:

4.1.1 EBOX GATEWAY (ZENTYAL GATEWAY)

Una de las funcionalidades principales de esta plataforma es precisamente la de ser configurada como puerta de enlace. Al configurar este modulo se puede realizar un balanceo de carga y disponibilidad para los casos en que se tenga más de una conexión a internet. De igual manera es posible distribuir los clientes conectados de forma transparente a pesar de que alguna de las conexiones se encuentre inactiva.

Ayuda a controlar lo que está ingresando a la red interna “Filtrado de

Contenidos", siendo este una de las principales preocupaciones de los gerentes dentro de las pequeñas organizaciones debido al uso inapropiado de los recursos de internet de sus trabajadores. Con lo cual se permite establecer y cumplir con las políticas de uso del internet.

Cache Transparente

Control de Trafico

Balanceo

Filtrado

Todas estas características son posibles gracias a la integración de diversas herramientas diseñadas para Linux. Algunas de ellas son:

Característica	**Software Integrado**
Firewall Avanzado	Netfilter
Enrutamiento Avanzado	Iprouter2
QoS(Calidad de Servicio) y Balanceo de Carga	L7filter – Iprouter2
Proxy HTTP – Filtrado de Contenidos y Antivirus	Squid, Dansguardian, ClamAV
Políticas de Usuarios, Grupos y Subredes	Squid
Servidor de Autentificación RADIUS	FreeRADIUS

Tabla 1. Características del Modulo eBox Gateway

4.1.1.1 Abstracciones de Red

La facilidad en la gestión del modulo Gateway radica en que es posible realizar abstracciones de la red a través de objetos que posteriormente serán utilizados en la configuración.

Objetos de red

Un objeto puede ser un elemento de la red o un grupo de elementos a los que posteriormente pueden aplicárseles políticas o reglas de control de acceso haciendo más fácil la configuración total.

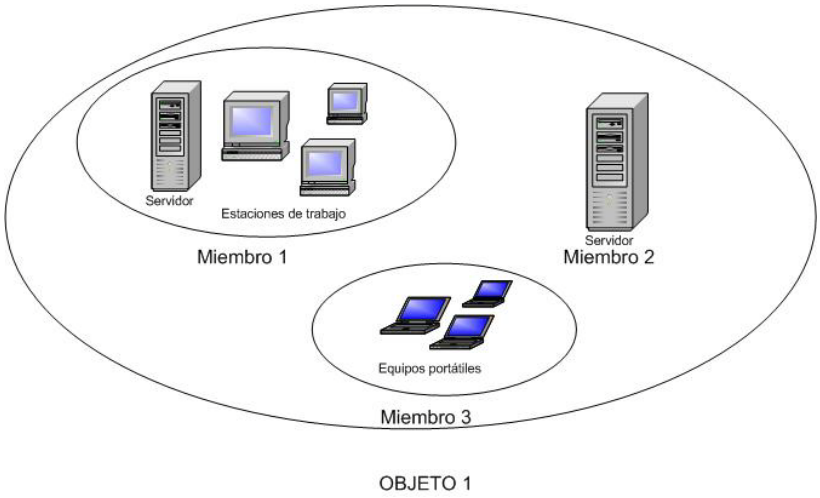


Figura 2. Representación de Objetos de Red

Servicios de Red

Un servicio de red es la abstracción de uno o de más protocolos de aplicación[6] que pueden ser usados en otros módulos como el cortafuego o el moldeado del tráfico[7].

El objetivo es representar a través de nombres los puertos que son usados por

[6] Protocolos de Aplicación: Son aquellos protocolos de alto nivel que posibilitan numerosas aplicaciones al usuario. Ejemplo: FTP, SMTP, DNS, HTTP, entre otras.

[7] Definición tomada de: http://doc.zentyal.org/es/1.2/abstractions.html#objetos-de-red

las aplicaciones para posteriormente facilitar la configuración al administrador debido a que es más fácil recordar los nombres que los números de los puertos.

En el modelo cliente/servidor, los servicios de red usan un puerto cualquiera aleatorio y se conectan a un puerto destino específico. Los puertos 1 al 1023 se llaman puertos bien conocidos, del puerto 1024 al 49151 se llaman puertos registrados y del puerto 49152 al 65535 se llaman puertos efímeros.

Algunos de los puertos llamados Bien conocidos se listan a continuación:

N. de puerto	Descripción
0	Reservado
1	**TCP** Servicio de multiplexado de puertos (TCPMUX)
20	**FTP** ("File Transfer Protocol") Datos
21	**FTP** ("File Transfer Protocol") Control
22	**SSH** Secure Shell Remote Login Protocol
23	**Telnet** (acceso a terminal remoto)
25	**SMTP** ("Simple Mail Transfer Protocol")
53	**DNS** ("Domain Name System")
69	**TFTP** ("Trivial File Transfer Protocol")
80	**WWW-HTTP** ("Hyper Text Transfer Protocol")
110	**POP3** ("Post Office Protocol")
113	**UDP** ("User Datagram Protocol")
115	**SFTP** ("Simple File Transfer Protocol")

143	**IMAP** ("Interim Mail Access Protocol")
156	SQL Server
161	**SNMP** ("Simple Network Management Protocol")
162	**SNMP** trap
389	**LDAP** ("Lightweight Directory Access Protocol")
443	**HTTPS** ("HyperText Transfer Protocol")
546	**DHCP** ("Dynamic Host Configuration Protocol") Cliente
547	**DHCP** Servidor
631	**UDP** ("User Datagram Protocol")

Tabla 2. Listado de Puertos Bien Conocidos

Tomado de : http://www.iana.org/assignments/port-numbers

4.1.1.2 Cortafuegos

Un cortafuego o firewall es un sistema que previene el uso y el acceso no autorizado a un computador o a una red. Su finalidad es reforzar las políticas de control de acceso entre las redes como por ejemplo asignar permisos a los usuarios para definir a que maquinas se puede conectar y a que información puede acceder o puede recibir. El cortafuegos en GNU/Linux se llama Netfilter.

Netfilter[8] es un framework disponible en el núcleo de Linux que permite interceptar y manipular paquetes de red, el componente más popular

[8] Tomado de: http://es.wikipedia.org/wiki/Netfilter/iptables

construido sobre Netfilter es iptables que adicionalmente permite realizar la traducción de direcciones de red NAT[9] para IPV4.

Cuando se configura EBOX como cortafuegos debe ser instalado entre la red local y el router (modem) que conecta esa red con internet. La interfaces de red que conectan la maquina con la red externa (Router) deben marcarse como tal, de este modo el cortafuegos establece unas políticas de filtrado por defecto que serán aplicadas automáticamente.

Existen cinco tipos de tráfico de red que pueden filtrarse con las reglas de filtrado en EBOX:

- Tráfico desde la red interna hacia el servidor EBOX.
- Tráfico desde la red interna hacia internet o entre redes internas si las hubiere. Un ejemplo práctico seria bloquear la salida a internet para una subred específica.
- Tráfico de EBOX a redes Externas (Navegación y descarga de archivos desde la maquina eBox)
- Tráfico de redes externas a eBox
- Tráfico de redes externas a redes internas. Acceder a un servidor Web interno desde Internet.

4.1.1.3 Enrutamiento

Enrutar hace referencia a decidir a través de cual interfaz se envía un paquete de datos que va a salir de una maquina. Los sistemas operativos incluyen una tabla de enrutamiento que define las reglas para tomar la decisión de hacia dónde van los paquetes, mínimamente incluye la regla de enrutamiento para la interfaz local (LoopBack “127.0.0.1”). La puerta de enlace es la ruta tomada en caso de no encontrarse otro camino que permita dar salida dentro de la tabla de rutas. Igualmente es la ruta por omisión cuando los paquetes que se van a transferir van hacia otras redes.

[9] Network Address Translation (NAT): Es el proceso de reescribir la fuente o destino de un paquete IP mientras pasan por un enrutador o cortafuegos. Su uso principal es permitir a varias máquinas de una red privada acceder a Internet con una única IP pública.

4.1.1.4 Reglas de Multirouter y Balanceo de Cargas

Una herramienta útil para las empresas donde se tiene más de una conexión ADSL que suministra Internet y se desea distribuir todo el ancho de banda de manera transparente es la regla de Multirouter. Con esta opción es posible distribuir la carga de manera automática. Por ejemplo clasificar el tráfico que se envía por uno de los router (Correo electrónico) y siempre enviarlo a través de una misma conexión.

eBox hace uso de iproute2 e iptables para implementar la funcionalidad de Multirouter. Al hacer uso de iproute2 se está informando al Kernel de Linux que existe más de un router y las reglas se pueden establecer gracias a Iptables.

El balanceo de carga consiste en repartir de manera equitativa los paquetes que salen hacia Internet. Esto se puede lograr dando pesos a cada router teniendo en cuenta la capacidad de cada uno de ellos, así se puede dar un mayor peso a la conexión de mayor ancho de banda y un menor peso a aquellas de menor capacidad. Con esto se hace un uso eficiente de los recursos.

4.1.1.5 Calidad de Servicio (QoS)

Hablar de Calidad de Servicio “Quality of Service” (QoS) en redes, es referirse a todos los mecanismos de control en la reserva de recursos para dar prioridad a los usuarios o a ciertos flujos de datos como multimedia o voz.

Existen diferentes técnicas para lograr QoS en redes. Entre ellas están:

Uso de Servicios Diferenciados (DiffServ): Esta técnica se basa en el marcado de paquetes de acuerdo al servicio al que están asignados. Con base a esas marcas, los enrutadores manejaran diferentes técnicas de colas. Actualmente esta técnica es bastante aceptada.

Algoritmos de Scheduling: Su propósito fundamental consiste en optimizar el rendimiento del Sistema Operativo.

Algoritmo de Modelado del tráfico mediante Token Bucket: [10] Este es un algoritmo de control de congestión basado en el conformado de tráfico. Es de tipo bucle abierto, lo que significa que previene la congestión (no reacciona cuando ya se ha producido, sino que previene que no se produzca), y lo hace conformando el tráfico que entra a la red para que ésta sea más determinista.

Evitación de la Congestión: Mediante el manejo de protocolos es posible evitar la congestión mediante el flujo de datos. Algunos de estos protocolos son: OSPF (Protocolo del Estado de Enlace), RIP (Protocolo de Vector Distancia)[11].

4.1.1.6 Servicio Proxy HTTP

Un proxy es un programa que realiza una acción en representación de otro. En este caso hace de intermediario entre la conexión de red y el protocolo HTTP.

eBox utiliza Squid[12] como proxy y además hace uso de Dansguardian[13] para el control de contenidos.

Entre las funcionalidades de este servicio se encuentran:

- Restricción de acceso dependiendo de un horario, usuario o dirección de origen.
- Actuar de caché de contenidos permitiendo una reducción en el consumo del ancho de banda

[10] Definición tomada de: http://www.it.uc3m.es/~prometeo/rsc/problemas/Examenes_uc3m/feb98/teoria~1/teoria~1.html#SOLp3
[11] Ver ampliación del concepto en el glosario.
[12] Ampliación de la definición: http://www.squid-cache.org/
[13] http://dansguardian.org/?page=whatisdg

- Antivirus y Filtro de contenidos.

4.1.2 EBOX UTM (ZENTYAL UTM) (UNIFIED THREAD MANAGER)

Permite implementar niveles de seguridad con la configuración de su cortafuegos. Esta configuración requiere de conocimiento en la creación de reglas de filtrado. Dentro de este se pueden encontrar el filtrado de paquetes y el redireccionamiento de Puertos.

Existe un sistema de detección de intrusiones, el cual informará cualquier intento de vulneración. Es posible configurar ciertas reglas para mejorar el sistema de seguridad sin embargo cuando se instala eBox vienen configuradas por defecto unas pocas reglas dentro de este sistema que pueden ser ampliadas.

También es posible mantener un buen nivel de seguridad en la comunicación entre oficinas geográficamente dispersas, esto se logra en eBox mediante la implementación de VPN (Virtual Prívate Networks)

En general la lista completa de las características del modulo UTM y el software que implementan se listan a continuación:

Característica	**Software Integrado**
Cortafuegos	Netfilter
Filtro de Correos	ClamAV, Spamassassin, Postgrev,Amavisd-newy, P3scan
Filtro Web (Análisis de Contenido, Listas Blancas, Listas Negras)	Squid, Dansguardian,ClamAV
Redes Privadas Virtuales (VPN)	OpenVPN
Sistema de Detección de Intrusos	Snort

Tabla 3. Características del Modulo eBox UTM

VPN Detección Intrusos Cortafuegos

4.1.2.1 Redes Privadas Virtuales (VPN)

Las redes privadas virtuales trabajan bajo un esquema de tunelización, en donde la información a transmitir se encapsula en datagramas IP y se enrutan a través de la red pública. Esta solución ofrece seguridad a un bajo costo, debido a que se pueden utilizar las conexiones de banda ancha y no se requieren de canales dedicados de datos que demanda un mayor costo.

Las VPN conectan usuarios a la red de la organización, cuando estos se encuentran fuera de ella, o también es posible conectar otras redes que se encuentren en sitios geográficamente distintos. Proporciona iguales beneficios y recursos que una red de área local.

En eBox las VPN utilizan la tecnología SSL (Secure Socket Layer), esta tecnología lleva bastante tiempo de uso (inicio en 1996) y adopta el uso de una infraestructura de clave pública PKI, donde se generan un par de claves: una publica y una privada. La clave pública se distribuye y es conocida por los destinatarios. Los datos se cifran con la clave pública y para descifrarlos solo es posible hacerlo con la clave privada.

4.1.2.2 Sistema de Detección de Intrusos

IDS (Sistema de Detección de Intrusos) es una aplicación que está diseñada para brindar seguridad. Opera monitorizando o detectando eventos que puedan llegar a comprometer la seguridad del sistema informático donde se

encuentra instalado o configurado (para el caso de una red), estos eventos son registrados en una base de datos o archivo.

Existen varios tipos de IDS, entre ellos:

- HIDS (Host IDS): Protegen contra un único servidor, Computador o Host. Funciona de modo local. Fueron los primeros IDS que se desarrollaron dentro de la industria de la seguridad informática.

- NIDS (Net IDS): Protege un sistema basado en red. Actúan sobre una red capturando y analizando paquetes de red. Son sniffers del tráfico de red. Luego analizan los paquetes capturados, buscando patrones que supongan algún tipo de ataque. Analizan el tráfico de red, normalmente, en tiempo real. No sólo trabajan a nivel TCP/IP, también lo pueden hacer a nivel de aplicación. Uno de los NIDS más popular es Snort[14] y es la herramienta que utiliza eBox para implementar la tarea de Detección de Intrusos. Snort implementa un motor de detección de ataques y barrido de puertos que permite registrar, alertar y responder ante cualquier anomalía previamente definida como patrones que corresponden a ataques, intentos de aprovechar alguna vulnerabilidad o análisis de protocolos conocidos.

4.1.3 EBOX INFRASTRUCTURE (ZENTYAL INFRASTRUCTURE)

Este modulo incluye servicios que permiten gestionar el trafico de la red interna. Incluye la configuración del servidor de dominio, la gestión de maquinas, el servidor web y la gestión de los certificados digitales además de la configuración del protocolo DHCP.

[14] Referencia: http://www.snort.org/

La aplicabilidad de utilizar o configurar un servidor de dominio se traduce en la facilidad de recordar un nombre en lugar de una dirección.

La lista completa de las características y el software que implementan se listan a continuación:

Característica	**Software Integrado**
Servidor DHCP	ISCDHCP[15]
Servidor DNS	BIND 9
Servidor NTP	Ntpd
Autoridad de Certificación	Open SSL
Servidor WEB	Apache
Servidor FTP	vsftpd

Tabla 4. Características del Modulo eBox Infraestructura.

4.1.3.1 Servicio de Configuración de Red DHCP:

eBox implementa ISCDHCP. Esta sigla define una colección de software que implementa todos los aspectos de la suite DHCP, esto es:

- Un servidor DHCP, el cual recibe las peticiones
- Un cliente DHCP, que está incluido en el sistema operativo de los equipos clientes y que envía peticiones al servidor DHCP.
- Un agente de retransmisión DHCP el cual pasa las peticiones de una LAN a otra de modo que no se requiere un servidor DHCP en cada LAN.

[15] Para más información de este servicio consultar: https://www.isc.org/software/dhcp

Al conectarse un cliente DHCP a la red, este envía una petición de difusión (Broadcast) y el servidor DCHP responde a esa petición con una dirección IP, el tiempo de concesión de la dirección IP, la puerta de enlace por defecto, la máscara de red, las direcciones IP de los servidores de nombres o el dominio. Esto facilita la tarea de los administradores de red ya que no requiere una previa configuración manual de los parámetros para ingresar a la red. Existen dos métodos de asignación de direcciones:

Manual: El administrador de la red se encargara de asignar las direcciones mediante tablas que deberá mantener actualizadas

Dinámico: El administrador asigna un rango de direcciones. El servidor guarda una tabla de asignaciones donde tratara siempre de asignar la misma dirección IP a un cliente en sucesivas ocasiones. El concepto de asignación se da bajo el modelo de alquiler por cierto periodo de tiempo. Este es el concepto que se maneja en DHCP.

4.1.3.2 Servidor DNS:

El espacio de nombres de dominio “DNS” tiene como funcionalidad convertir las direcciones IP a nombres de maquinas que son más fáciles de recordar y de igual manera traduce los nombres a direcciones IP. Este sistema presenta una arquitectura jerárquica en forma de árbol cuyo objetivo es evitar la duplicación de información y facilita la búsqueda de dominios. Este servicio utiliza el puerto 53 y opera sobre protocolos TCP y UDP.

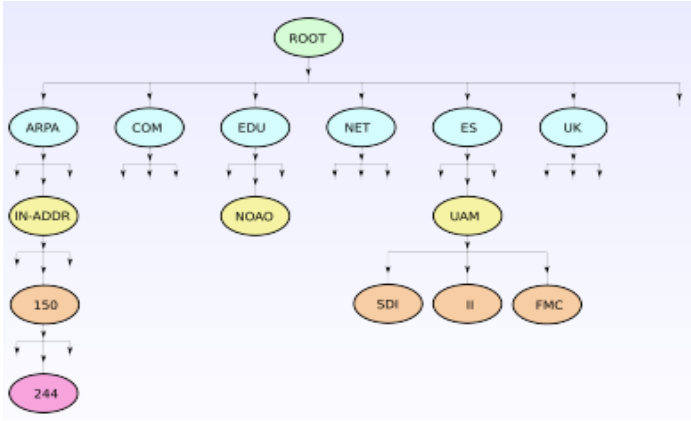


Figura 3 DNS: Arquitectura Jerárquica en Forma de Árbol

Tomado de: http://memnon.ii.uam.es/~eloy/media/REDES/Tema7.1-DNS.pdf

4.1.3.3 Servidor NTP

Network Time Protocol. Este protocolo fue diseñado para sincronizar los relojes de los equipos en redes no fiables con latencia variable. Opera sobre el puerto 123 bajo el protocolo UDP y es uno de los protocolos más antiguos de internet

4.1.3.4 Servidor WEB

Cuando se habla de WEB se hace referencia al protocolo HTTP (Hyper Text Transfer Protocol). Este protocolo está orientado a peticiones y respuestas, donde un cliente realiza una petición a un servidor y el servidor procesa la solicitud y devuelve una respuesta. El puerto usado por este protocolo es el puerto 80 para conexiones sin cifrar y para conexiones cifradas usa el puerto 443 (HTTPS). Opera sobre TCP[16].

4.1.3.5 Servidor HTTP Apache

Este software es utilizado muy ampliamente por grandes empresas, instituciones educativas, organizaciones pequeñas, personas

[16] Protocolo TCP está orientado a conexión. Este protocolo garantiza que los datos serán entregados en su destino sin errores y en el mismo orden en que se transmitieron.

particulares. Es usado por eBox tanto para su interfaz de administración grafica como en el modulo Web.

4.1.4 EBOX OFFICE (ZENTYAL OFFICE)

El modulo de Oficina permite gestionar los recursos de la red tales como Archivos, Impresoras, Tareas, Backups de Datos por red, permite manejar perfiles de usuarios y grupos (Creando Grupos por cada departamento de trabajo o un único grupo que reúna a todos los computadores de la organización) todo administrado desde un mismo sitio y facilitando el manejo de permisos sobre los datos.

Una ventaja para los administradores de la red consiste en que es posible automatizar los Backups de datos lo que permite evitar inconvenientes por fallos de discos o por mala manipulación de la información por parte de los usuarios (Borrado accidental de archivos)

Todas las Características implícitas de este modulo y el software que implementan se listan a continuación:

Característica	**Software Integrado**
Servidor LDAP (administración centralizada de usuarios y grupos, arquitectura maestro/esclavo)	Open LDAP
Autenticación centralizada, incluyendo Controlador Primario de Dominio (PDC), sincronización con Active Directory (AD) y Perfiles Móviles.	Samba
Compartición de calendarios, Contactos y Tareas (Groupware)	Zarafa

Compartición de Carpetas y Archivos	Samba
Compartición de Impresoras	Cups
Backup de Datos	Duplicity

Tabla 5. Características del Modulo eBox Office.

4.1.4.1 Servicio de Directorios LDAP

LDAP (Lightweight Directory Acces Protocol- Protocolo Ligero de Acceso a Directorios) es un protocolo de tipo cliente-servidor para acceder a un servicio de directorio. Un servicio de directorios es utilizado para almacenar y organizar información concerniente a una organización: Usuarios y Grupos. Son ejemplos de servicios de directorio el Microsoft Active Directory (Windows), el Novell Directory Service (Novell) y el Network Information Service"NIS" de SUN Microsystem.

eBox usa OpenLDAP como servicio de directorio y hace uso de SAMBA como controlador de dominio para los usuarios Windows y también para el manejo compartido de archivos e impresoras.

4.1.4.2 Servicio de Archivos Compartidos y de Autenticación

Para compartir archivos y autenticar usuarios Windows en eBox se hace uso de Samba. Esta utilidad viene integrada con el modulo de usuarios y grupos, donde cada usuario tiene su directorio personal y cada grupo comparte su directorio con los usuarios que pertenecen a dicho grupo.

4.1.4.3 Compartición de Impresoras

La gestión de impresoras se da gracias al protocolo Samba, pero también es posible habilitar el demonio de impresión CUPS que permitirá acceder a las impresoras mediante el protocolo IPP (Internet Printing Protocol). Cups es un sistema modular de impresión para sistemas Unix que le permite a una

maquina actuar como servidor de impresión. Cuando no se dispone de un controlador para eBox de una impresora, es necesario habilitar CUPS.

4.1.5 EBOX COMUNICACIONES UNIFICADAS (ZENTYAL UNIFIED COMUNICATIONS)

Al hablar de comunicaciones unificadas se hace referencia a que es posible acceder a diferentes métodos de comunicación para compartir información haciendo uso del mismo nombre de usuario y contraseña para todos ellos. Entre estos métodos de comunicación se encuentra el correo electrónico, el servicio de mensajería instantánea y la voz sobre IP.

4.1.5.1 Servicio de Voz sobre IP

El concepto de voz sobre IP consiste en transmitir voz sobre redes de datos utilizando una serie de protocolos para enviar la señal digital en paquetes en lugar de utilizar las redes de circuitos analógicos conectados. Este servicio requiere de aplicar reglas de QoS tomando a consideración la latencia (tiempo que tarda en llegar al destino), el Jitter (Variación de la latencia) y el ancho de banda.

Son varios los protocolos que intervienen en el servicio de transmisión de voz a través de la red de Datos, tanto para la señalización como para el transporte.

Las tareas asignadas a los protocolos de señalización para Voz sobre IP son las de establecimiento y control de las llamadas. Entre ellos se encuentran: SIP, IAX2 Y H.323

Las tareas del protocolo de transporte consisten en transportar la voz codificada desde el origen hacia el destino. El más utilizado es el RTP “Realtime Transport Protocol”

5 MANUAL DE CONFIGURACION VERSION 1.0

5.1 INSTALACIÓN EN VIRTUAL BOX

La configuración inicial de la plataforma se hace sobre una instalación en maquina virtual donde se realizaran las pruebas totales de configuración y posteriormente se podrá replicar todo en una maquina servidora. La herramienta a utilizar es Virtual Box (de ORACLE)[17], donde se realizara la instalación de un sistema Linux – Versión Ubuntu.

Existen dos formas de crear la maquina virtual:

1. Hacer la instalación desde cero. Esto conlleva a crear la imagen del disco y posteriormente configurar la plataforma eBox.
2. Hacer uso de una imagen ya creada de la plataforma eBox, donde no hacemos parte de la instalación.

Para el desarrollo de este manual se detallara la forma número 1, con esto se facilitara la instalación posterior en Hardware físico.

Al iniciar el Virtual Box se debe crear una nueva máquina virtual

[17] Sitio de descarga : http://www.virtualbox.org/wiki/Downloads

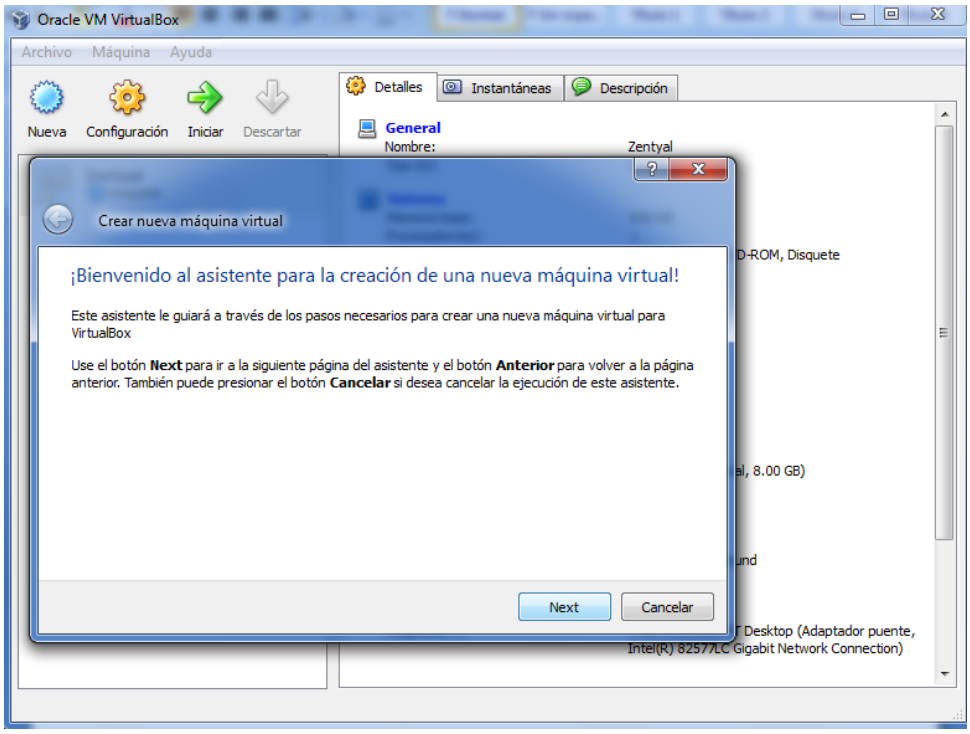


Figura 4. Inicialización Maquina Virtual –Virtual Box-

Se asigna un nombre y se selecciona el sistema operativo que se quiere instalar. Para el uso de eBoxPlatform se debe utilizar Linux-Version Ubuntu

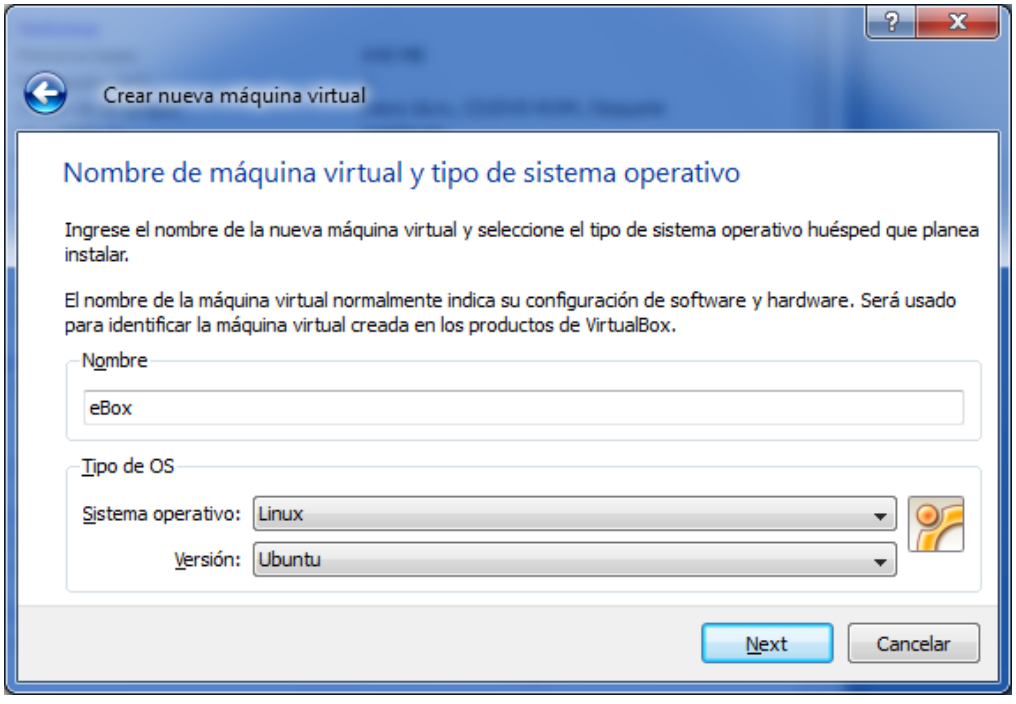
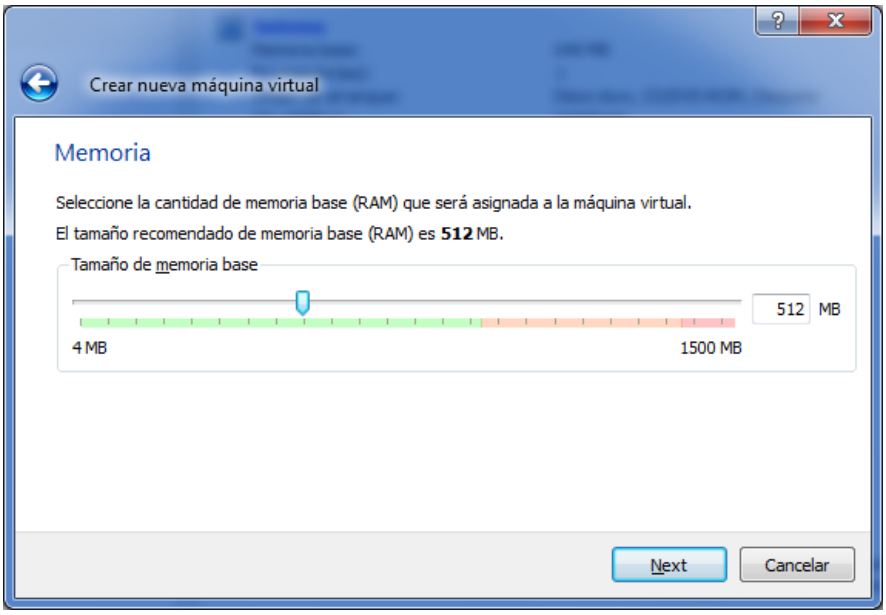


Figura 5. Formulario selección S.O a instalar

Se asigna la memoria al sistema (para las pruebas es suficiente 512MB, sin embargo si se dispone de gran capacidad de memoria en la maquina anfitriona es posible asignar más memoria.



Se crea un nuevo disco. Este nuevo disco va a tener un espacio dinámico que irá creciendo hasta la capacidad que se defina.

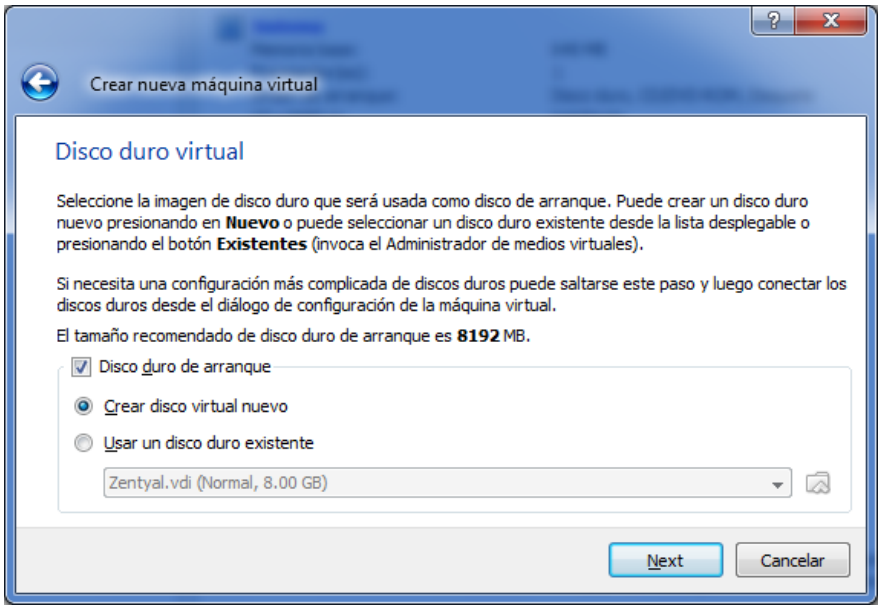


Figura 6. Creación del Disco Duro Virtual

Para una configuración básica de eBox es suficiente asignar 10 GB

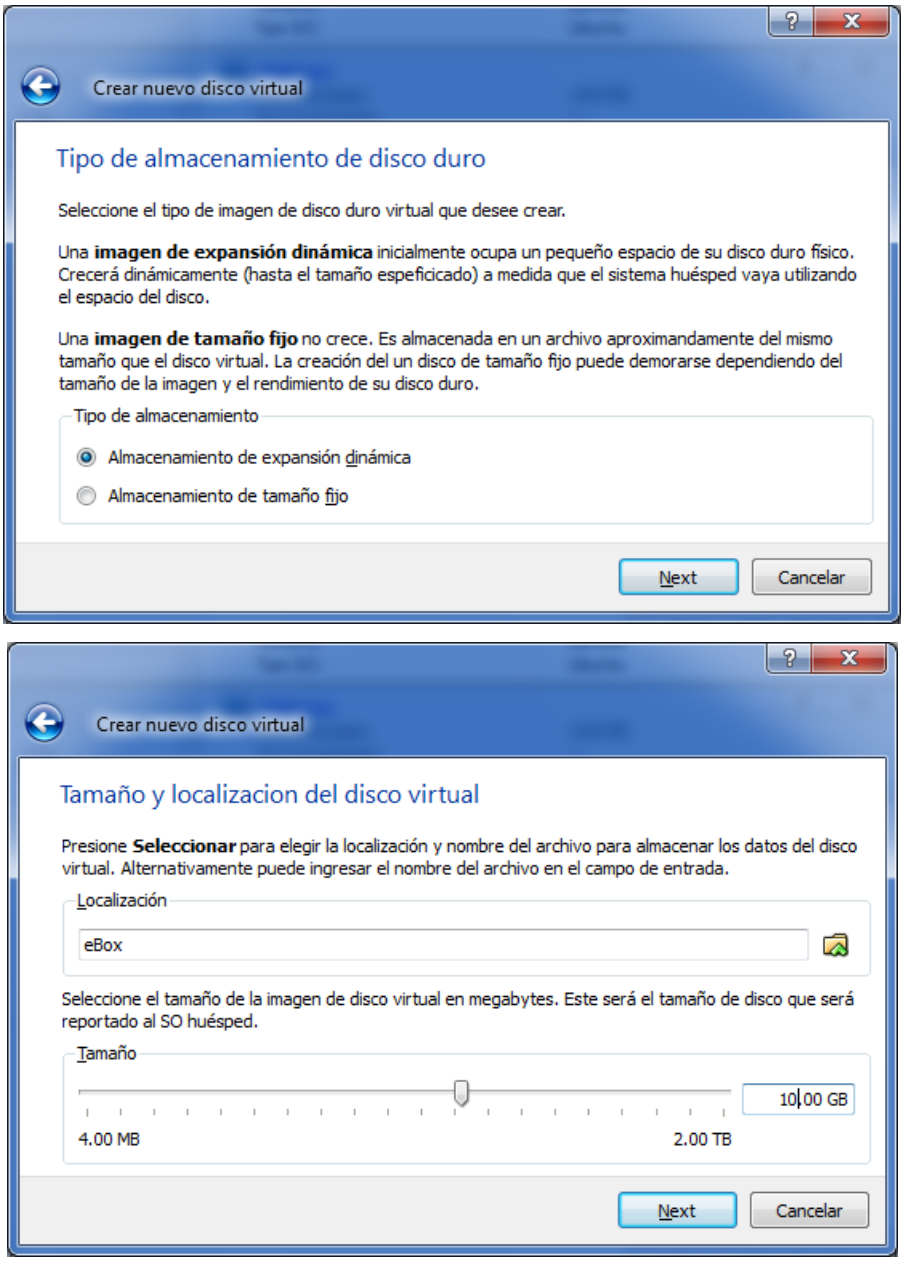
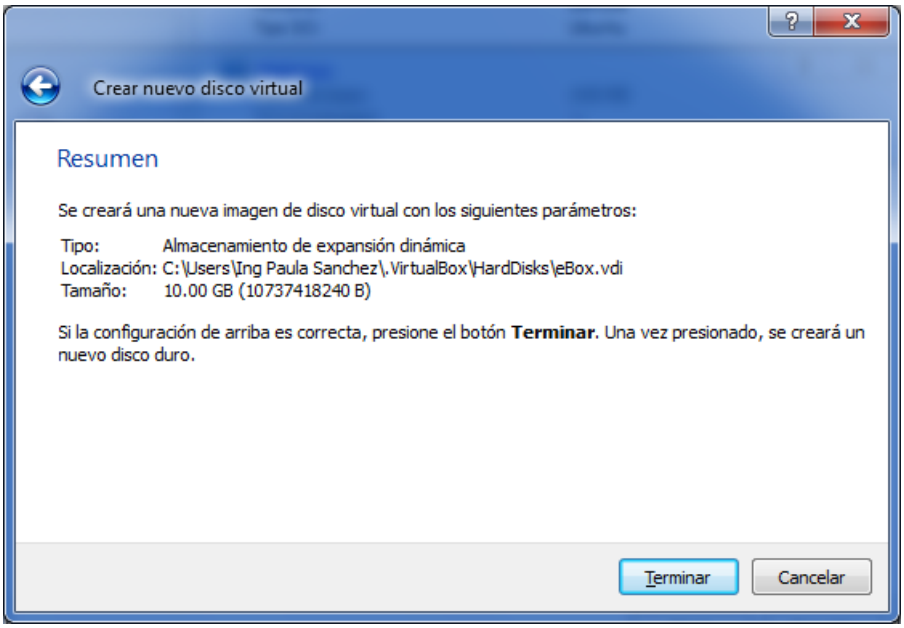


Figura 7. Asignacion de espacio para Disco duro en VirtualBox



5.1.1 CONFIGURACIONES GENERALES

Una vez terminado el procedimiento se pasa a configurar los aspectos generales de la maquina creada. Para hacer esto se selecciona la maquina y se da clic en el icono/botón de configuración:

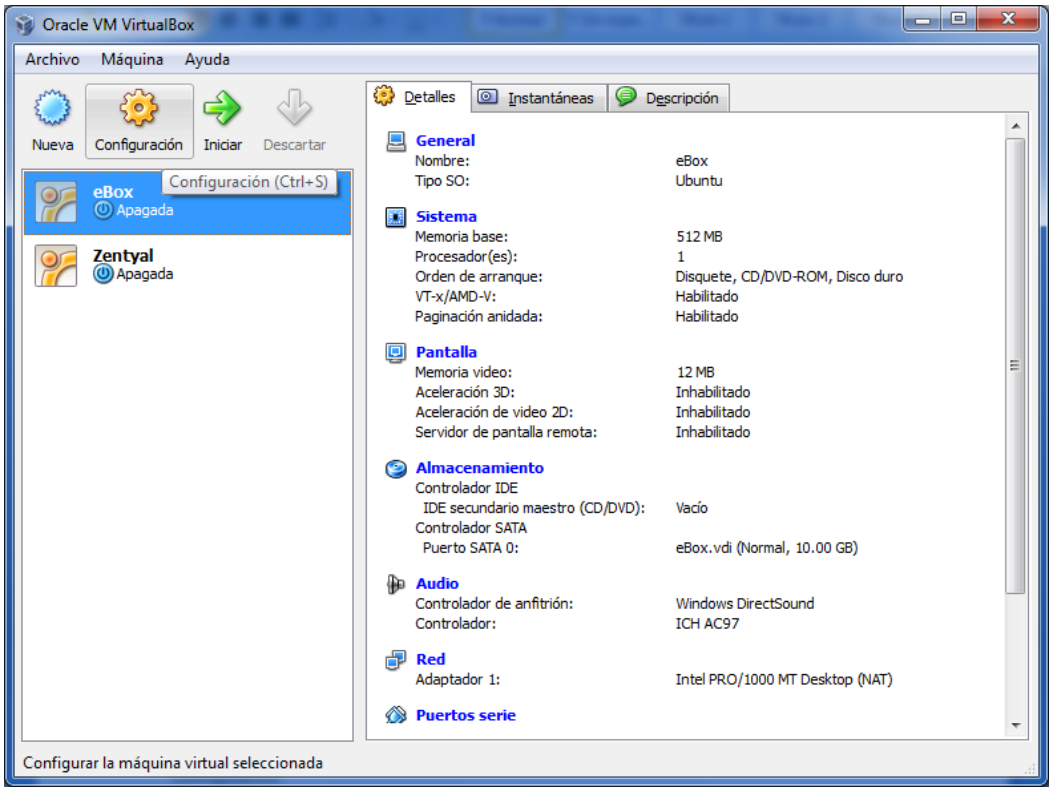
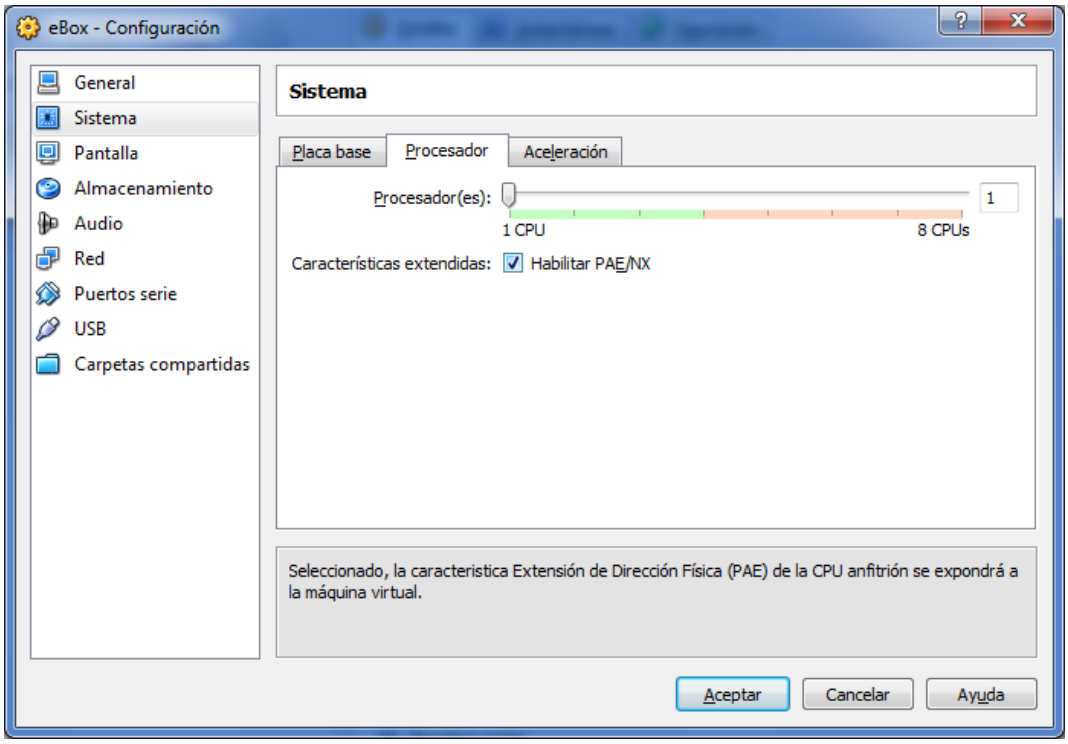


Figura 8. Interfaz Principal VirtualBox

Se despliega una ventana donde es posible configurar los detalles generales de la configuración.

Para que eBox corra en esta máquina virtual es necesario configurar dentro del modulo de sistema, en la pestaña del procesador las características extendidas, esto es marcar el checkbox “Habilitar PAE/ NX”[18] (Esto se hace para que eBox funcione sobre Virtual Box)

[18] Ampliación del concepto en el Glosario



5.1.2 ALMACENAMIENTO EN DISCO

Lo siguiente a configurar es el modulo de almacenamiento. El disco físico se crea en el momento de instalar el Virtual Box, pero debemos adicionar la unidad de CD desde donde se va a instalar la nueva plataforma, inicialmente el controlador IDE se encuentra vacio,

En la seccion de Atributos, es posible asignar la unidad que se desea utilizar. Para este caso se selecciona la unidad G que es una unidad virtual de CD del sistema anfitrion donde se va a montar la imagen iso de la plataforma eBox.

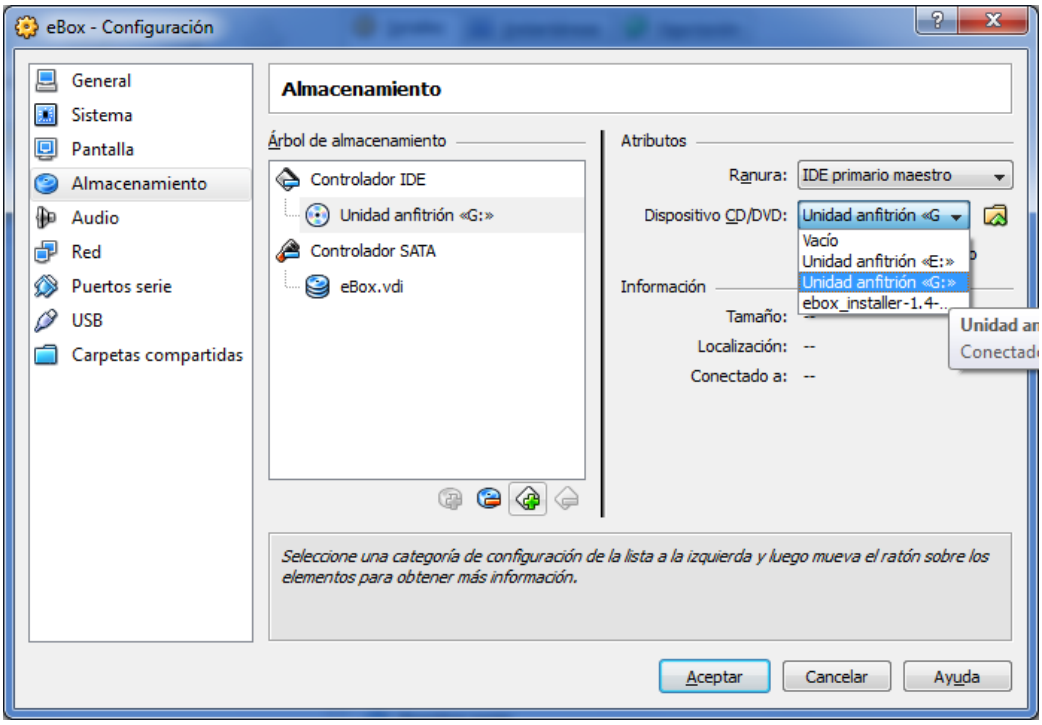


Figura 9. Selección de unidad de CD para la maquina Virtual

5.1.3 CONFIGURACIÓN DE ADAPTADORES DE RED

Lo siguiente es configurar el modulo de red, es importante tener en cuenta que si queremos tener conectividad entre la maquina anfitriona (maquina física) y la maquina huésped (maquina virtual) la tarjeta de red debe quedar configurada en modo puente.

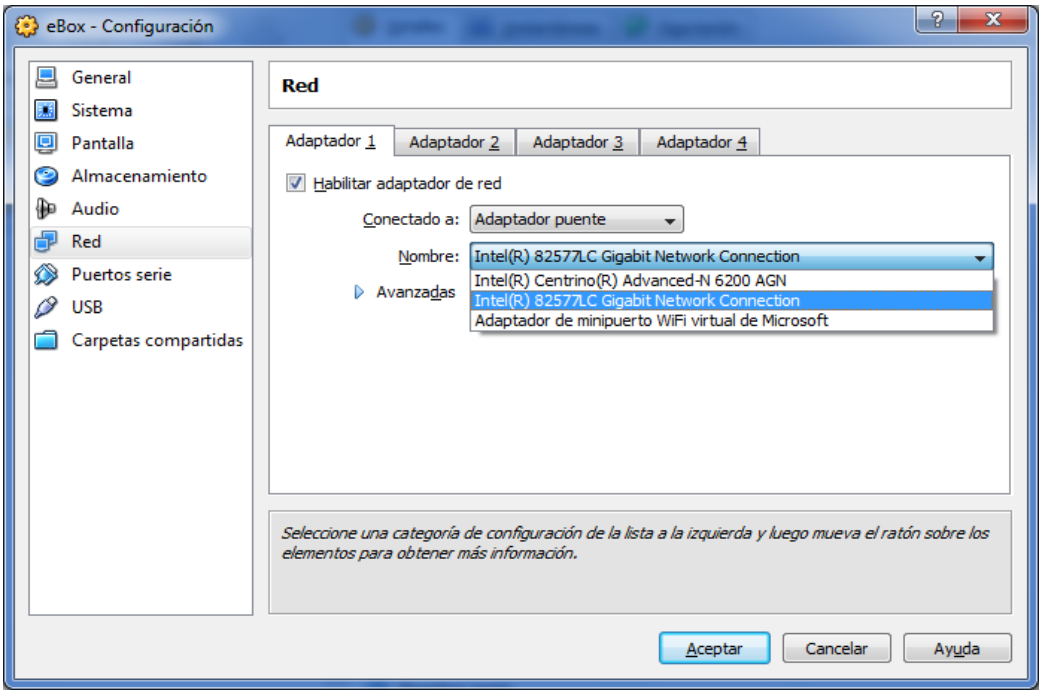


Figura 10. Selección de Tarjeta de red para la maquina Virtual

Para el ejemplo se selecciona la tarjeta de red Intel (R) 8257LC Gigabit Network Conexión que corresponde al adaptador de red Ethernet de la maquina anfitriona. Una vez finalizada la configuración. Se procede a montar la imagen del instalador de eBox en la unidad de CD virtual de la maquina anfitriona para después iniciar la maquina virtual.

5.1.4 INICIO DE LA INSTALACIÓN

Se inicia la instalación de eBox con la selección del idioma en que se desea instalar y se presentan las opciones de instalación.

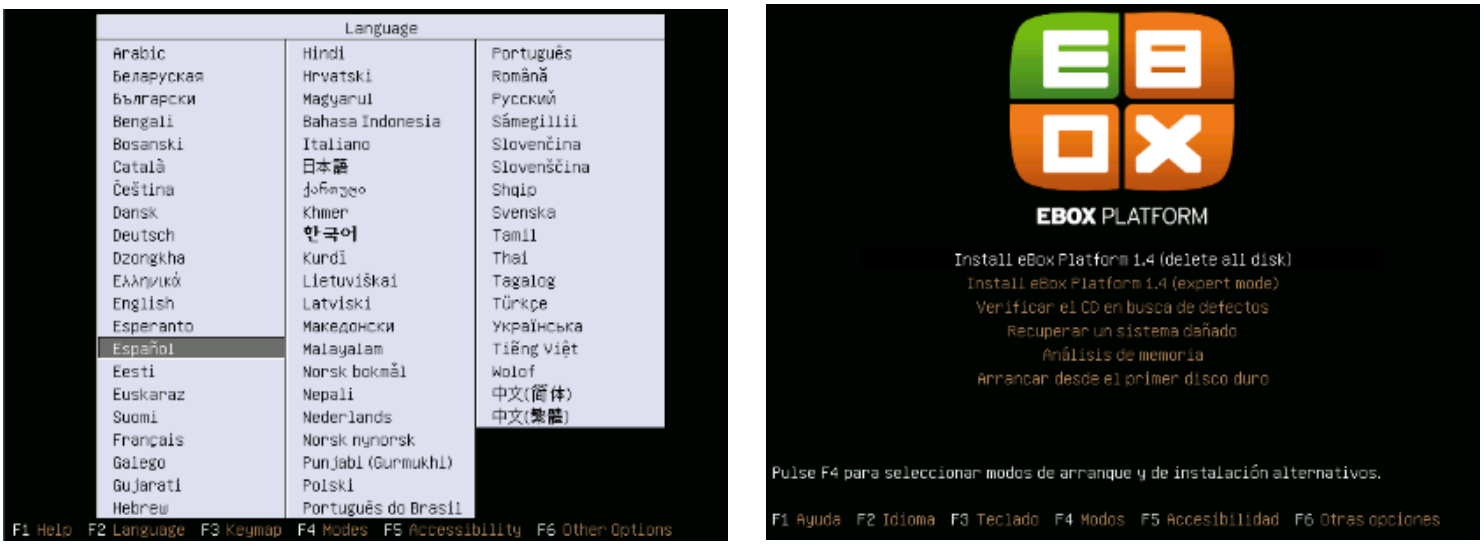
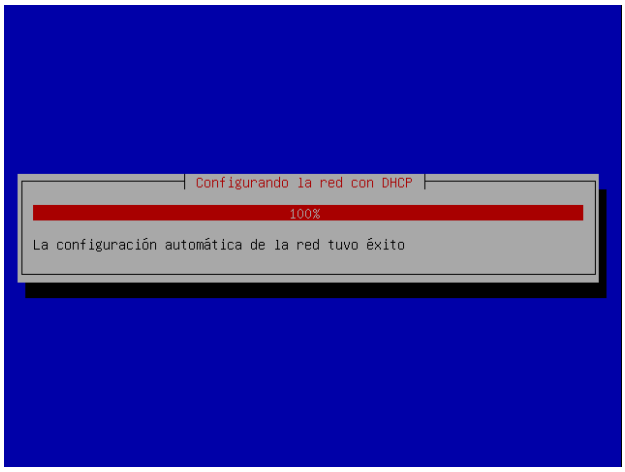


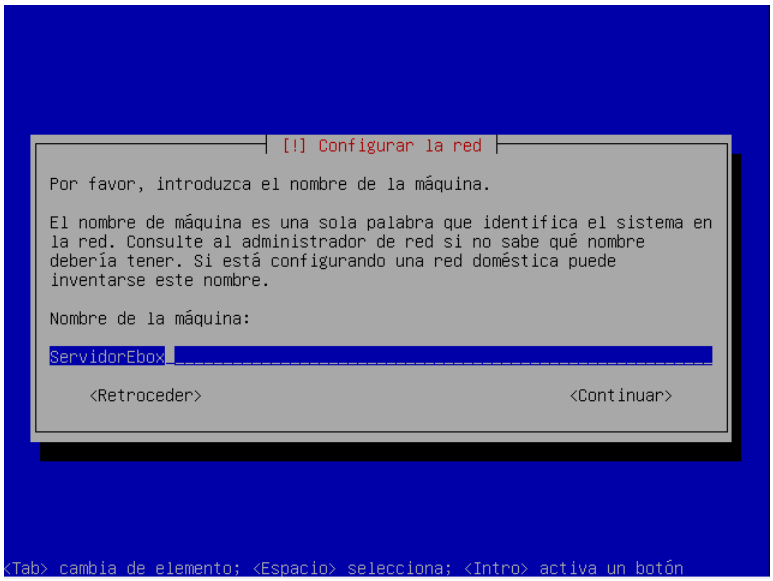
Figura 11. Imágenes de la instalación EBox en la maquina virtual

Para este caso como se tiene la imagen del disco vacía, se puede seleccionar la primera opción donde el proceso de instalación borra todo el disco. Además facilita la instalación pues no exige conocimiento previo de la plataforma (Un modo experto).

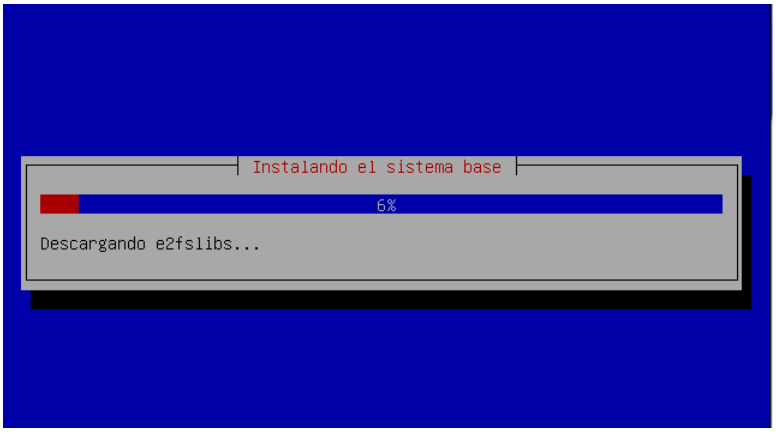
A continuación se configura la región: Para nuestro caso Colombia, después de esto el instalador verifica el estado del CD e inicia la configuración con el adaptador de red.

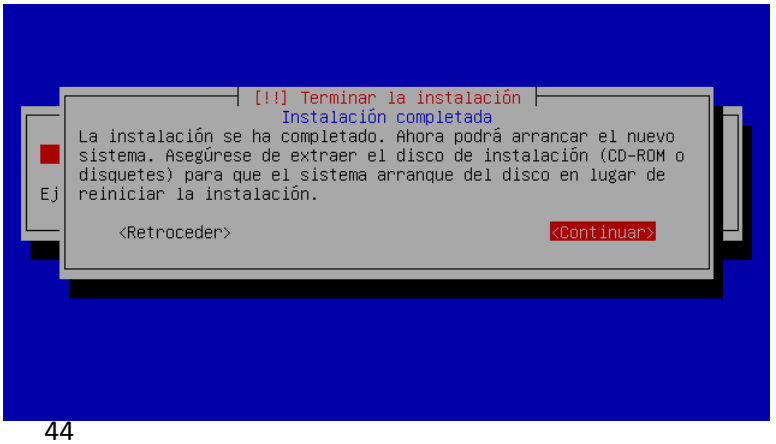


Se le debe asignar el nombre de la maquina:



e inicia la instalacion del sistema base





Es posible seleccionar los módulos a instalar de forma simple o avanzada. El modo simple consiste en seleccionar cada uno de las tareas que se quieren configurar y se instalan completas de forma automática y el modo avanzado permite instalar solo las opciones que se consideren necesarias.

En este caso para facilitar la configuración se seleccionaran los paquetes por tarea, de esta forma se asegura que no existan faltantes en la instalación según la tarea seleccionada. Además facilita la instalación para aquellos usuarios que apenas inician la exploración de esta plataforma. Sin embargo en el modo avanzado es posible instalar posteriormente cualquier paquete que no haya sido instalado o desinstalar alguno que no sea requerido.

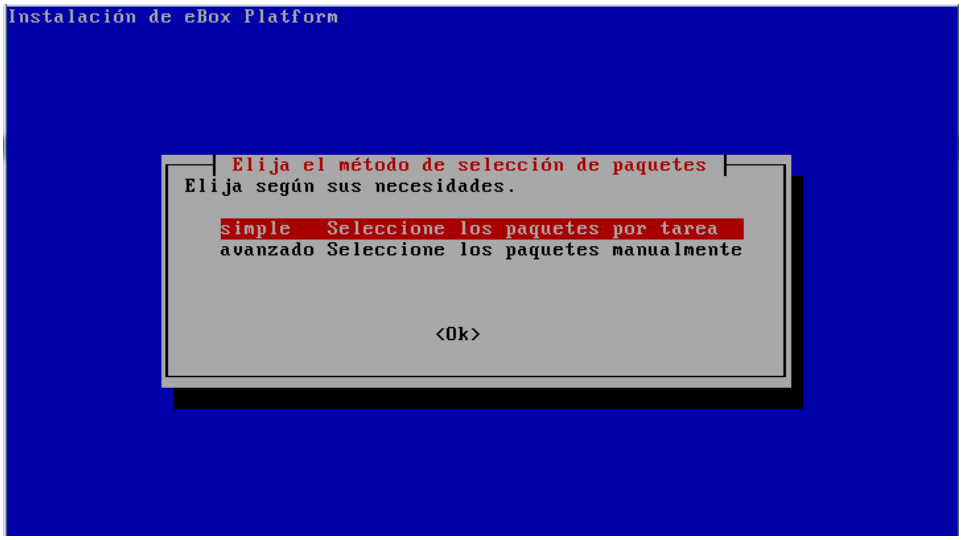
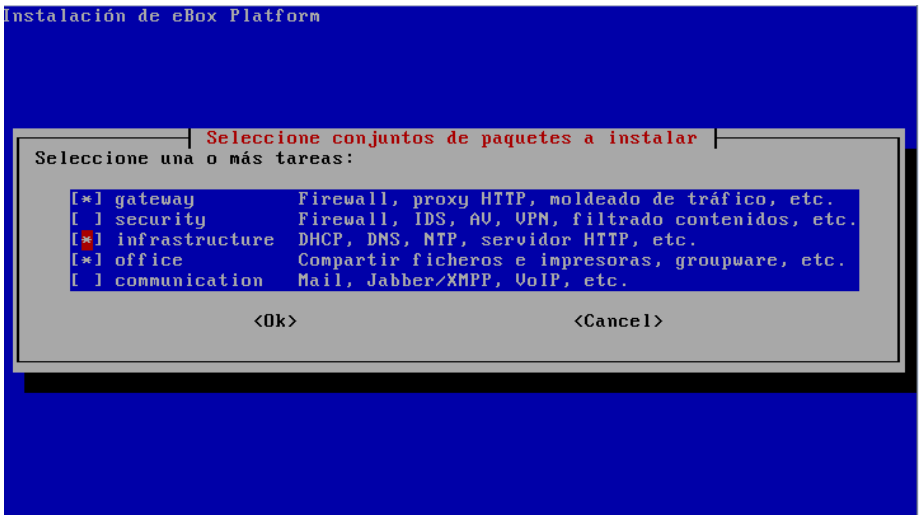


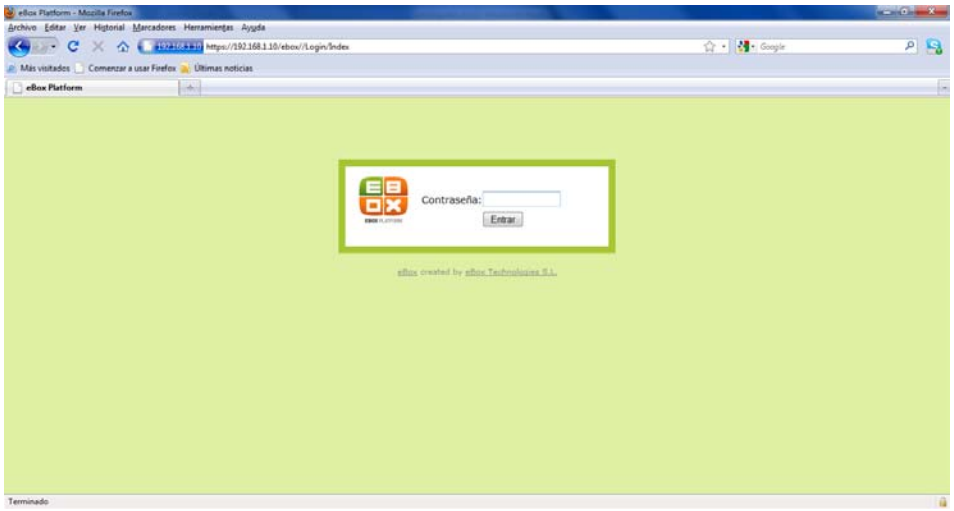
Figura 12. Selección del modo de instalacion de EBox

Los paquetes que se instalaran son los que corresponden a los modulos: Gateway, Infraestructure y Office. Posteriormente esta misma configuracion se replicará en el Servidor fisico dentro de la organización.



Una vez finalizado este procedimiento, será posible acceder a la interfaz web de administración previa identificación del usuario creado como administrador. Como estamos trabajando en una maquina virtual, es posible acceder a la interfaz web desde la maquina anfitriona. Para ello se debe usar el navegador Mozila Firefox y colocar la dirección IP que hayamos registrado en el momento de la instalación. En este caso la dirección fue 192.168.1.10

5.1.5 INTERFAZ WEB DE ADMINISTRACIÓN EN EBOX (ZENTYAL)



Al acceder con la contraseña establecia para el administrador durante la instalacion, se muestra la interfaz principal de eBox.

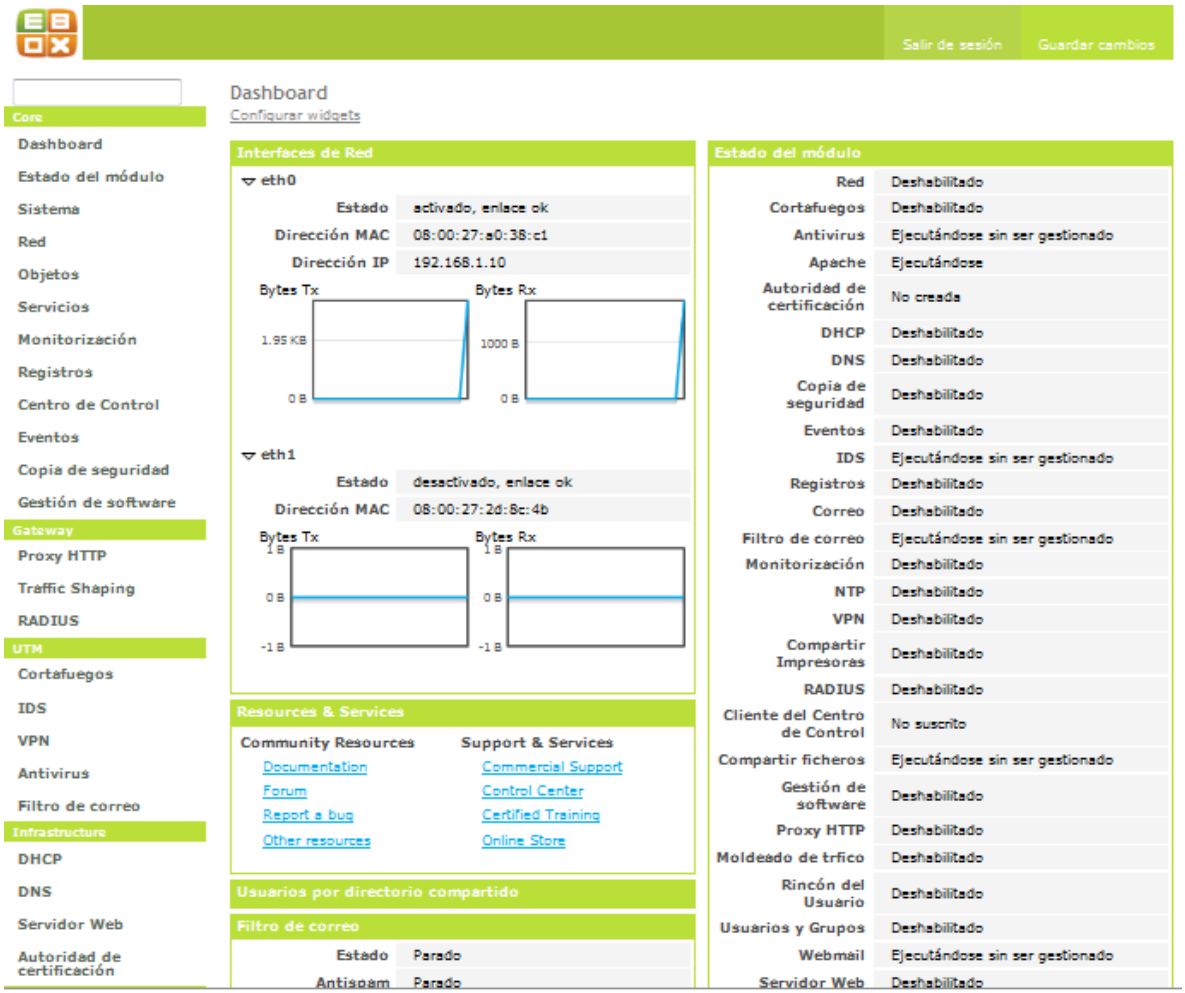
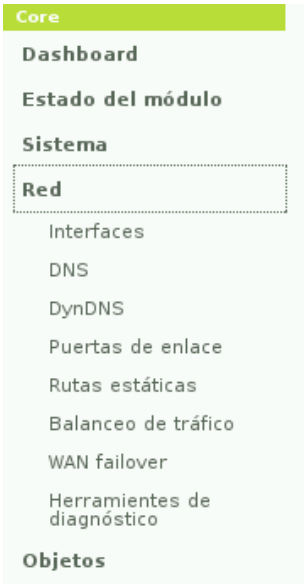


Figura 13. Interfaz Principal de EBox Platform

La interfaz principal está dividida en tres partes:

1. El menu lateral izquierdo corresponde a los servicios que se pueden configurar en el servidor



Al seleccionar alguno de estos servicios es posible que se despliegue un submenú donde se pueden configurar parámetros correspondientes a dicho servicio (Ejemplo: Servicio de Red- Al seleccionar se despliega el submenú donde se puede acceder a las Interfaces de Red- configuración DNS – configuración de la Puerta de enlace- etc).

2. El menú superior que corresponde solo a dos acciones: Salir de la sesión o Guardar cambios (Se colocara en color rojo cada vez que ocurra algún cambio en la configuración).

3. La zona central que comprende uno o varios formularios o tablas con información acerca de la configuración del servicio seleccionado a través del menú lateral izquierdo y sus submenús.

La primer interfaz que se muestra en el servidor es el Dashboard, allí se encuentran una serie de widgets (aplicaciones) configurables que pueden ser usadas en cualquier momento.

Esta interfaz principal permite explorar el estado de los módulos o servicios que se encuentran ejecutándose en el servidor. Para ello es necesario ingresar a la

segunda opción del menú lateral izquierdo “Estado del Modulo” y en la zona central se mostrara la información relativa. Un modulo puede presentar cuatro estados diferentes:

Ejecutándose: El servicio se está ejecutando aceptando conexiones de los clientes.

Ejecutándose sin ser gestionado: Si no se ha activado todavía el módulo, se ejecutará con la configuración por defecto de la distribución.

Parado: El servicio está parado bien por acción del administrador o porque ha ocurrido algún problema. Se puede iniciar el servicio mediante *Arrancar*.

Deshabilitado: El módulo ha sido deshabilitado explícitamente por el administrador.

El estado inicial de los modulos para nuestra maquina virtual se muestra de la siguiente forma:

Estado del módulo	
Red	Deshabilitado
Cortafuegos	Deshabilitado
Antivirus	Ejecutándose sin ser gestionado
Apache	Ejecutándose
Autoridad de certificación	No creada
DHCP	Deshabilitado
DNS	Deshabilitado
Copia de seguridad	Deshabilitado
Eventos	Deshabilitado
IDS	Ejecutándose sin ser gestionado
Registros	Deshabilitado
Correo	Deshabilitado
Filtro de correo	Ejecutándose sin ser gestionado
Monitorización	Deshabilitado
NTP	Deshabilitado
VPN	Deshabilitado
Compartir Impresoras	Deshabilitado
RADIUS	Deshabilitado
Cliente del Centro de Control	No suscrito
Compartir ficheros	Ejecutándose sin ser gestionado
Gestión de software	Deshabilitado
Proxy HTTP	Deshabilitado
Moldeado de trfico	Deshabilitado
Rincón del Usuario	Deshabilitado
Usuarios y Grupos	Deshabilitado
Webmail	Ejecutándose sin ser gestionado
Servidor Web	Deshabilitado

Figura 14. Estado de los Módulos dentro de EBox

De este listado vamos a cambiar algunos módulos que forman parte de las funcionalidades de Gateway, Office e Infraestructura, que serán utilizados en la organización VITELSA S.A.

5.2 CONFIGURACIÓN DEL SERVIDOR EBOX (ZENTYAL)

5.2.1 ACTIVACION DE LOS MODULOS DENTRO DE EBOX

Lo primero que se debe hacer en ubicarnos en el menú lateral izquierdo, dar click a la opción “Estado del Modulo”. Automáticamente se muestra en la zona central el formulario correspondiente al listado. Allí es posible activar los servicios requeridos:

Figura 15. Activacion de Modulos requeridos para la configuración

En esta imagen se encuentra sombreado dentro del recuadro rojo los aspectos relevantes ya mencionados. Las casillas de verificación (Check-Box) correspondientes a la columna Estado, se usan para marcarlas y automáticamente activar el modulo seleccionado.

Cuando se marca o activa un modulo, un mensaje se muestra informando los cambios que ocurrirán en la configuración del sistema Linux.

Iniciamos entonces activando el modulo de red que es el modulo principal para las tareas de configuración de Infraestructura. Al hacerlo surge un formulario emergente donde se reportan las modificaciones que se realizaran automáticamente dentro de los archivos de configuración del sistema Linux y debemos aceptar esos cambios para poder habilitar dicho modulo.

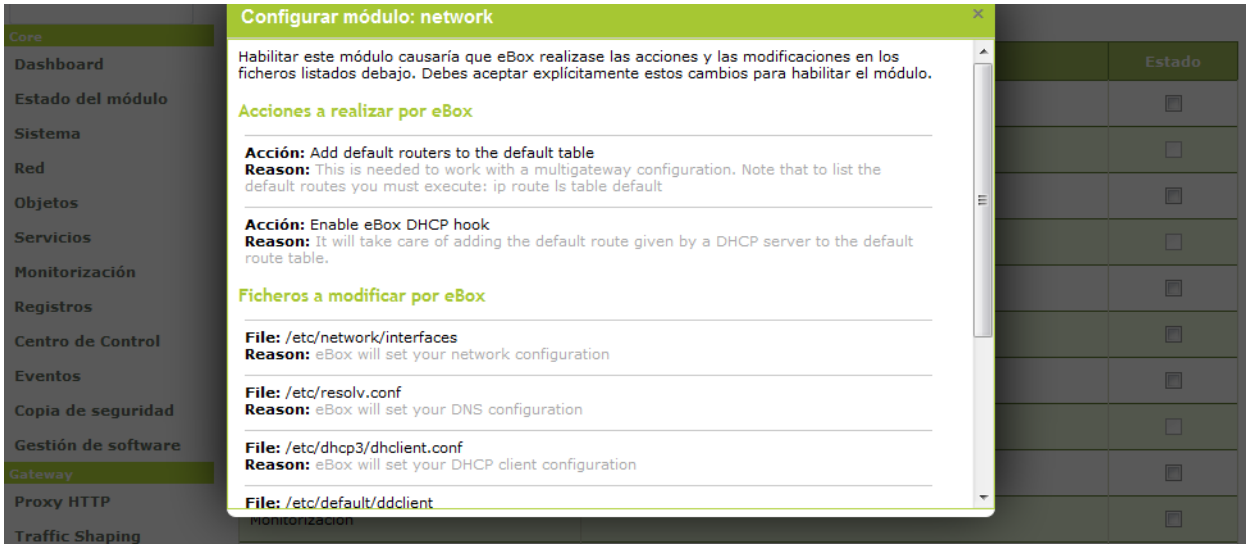
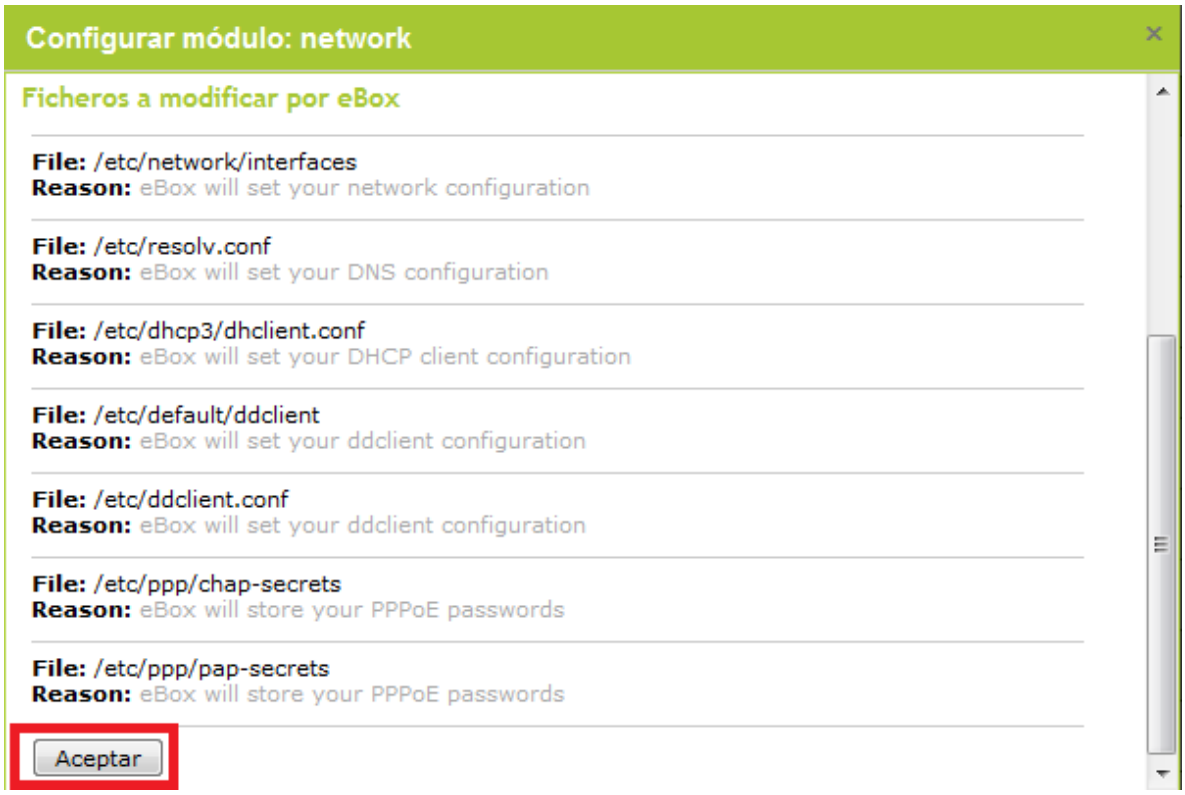


Figura 16. Configuración del Modulo de Red. Cambios automáticos.



Al dar clic en el botón Aceptar, automáticamente eBox cambia el estado del modulo, pero debemos guardar los cambios para que sean definitivos. Para ello se debe dar click en el Botón “Guardar Cambios” del menú superior que se encuentra ahora de color rojo, como señal que algo ha cambiado. En caso contrario el sistema no ejecuta ningún cambio.

Figura 17. Boton Guardar cambios cambia de color al ocurrir modificaciones.

Ahora se debe habilitar cada uno de los módulos que interesan para las tareas del servidor principal:

Office:

- Usuarios y Grupos
- Compartir Carpetas

Gateway:

- Proxy HTTP
- Balanceo de Carga
- Wan Fail Over (Pruebas de verificación para el balanceo de cargas)

A continuación las imágenes de los formularios emergentes para cada uno de los momentos de activación según los módulos:

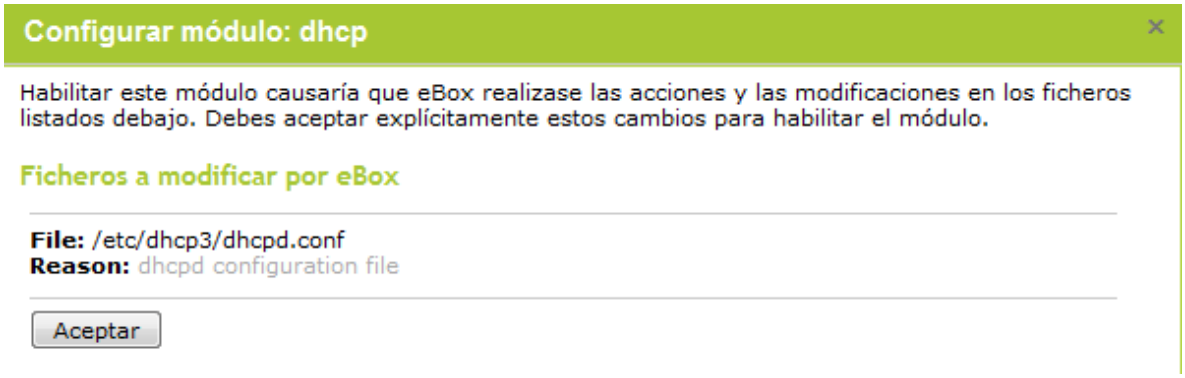


Figura 18. Formulario emergente al Activar el Módulo DHCP

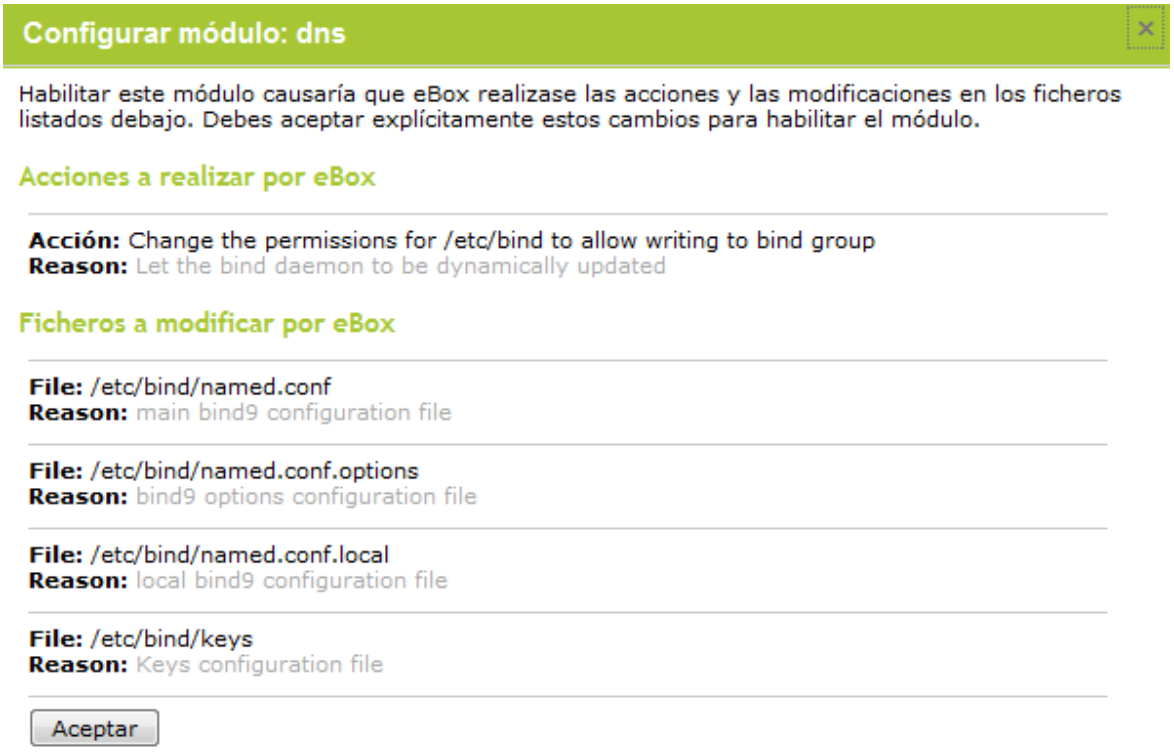


Figura 19. Formulario emergente al Activar el Módulo DNS

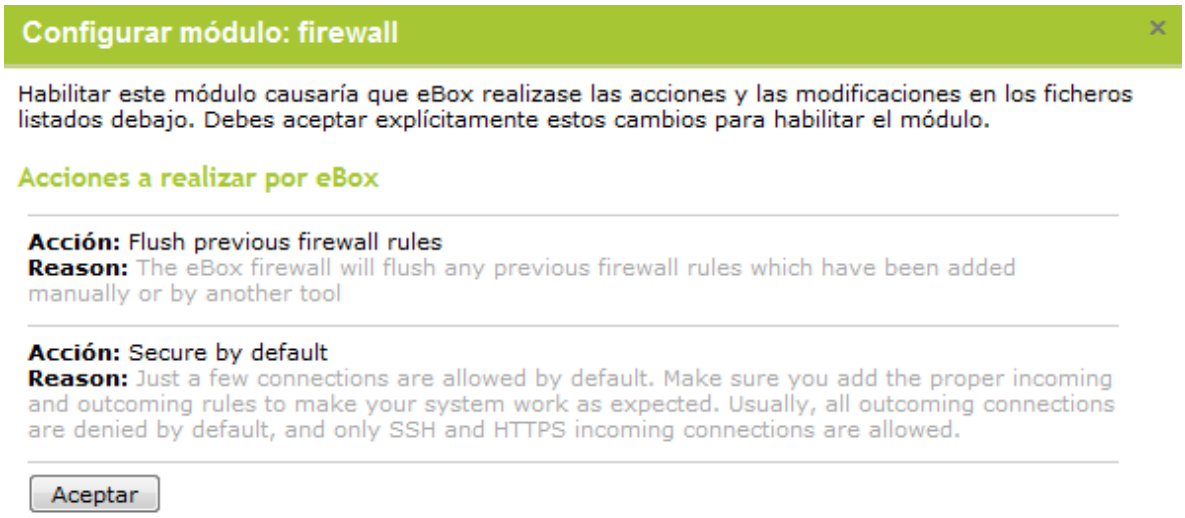


Figura 20. Formulario Emergente al Activar el Cortafuegos

Figura 21. Formulario Emergente al Activar el Módulo Usuarios y Grupos

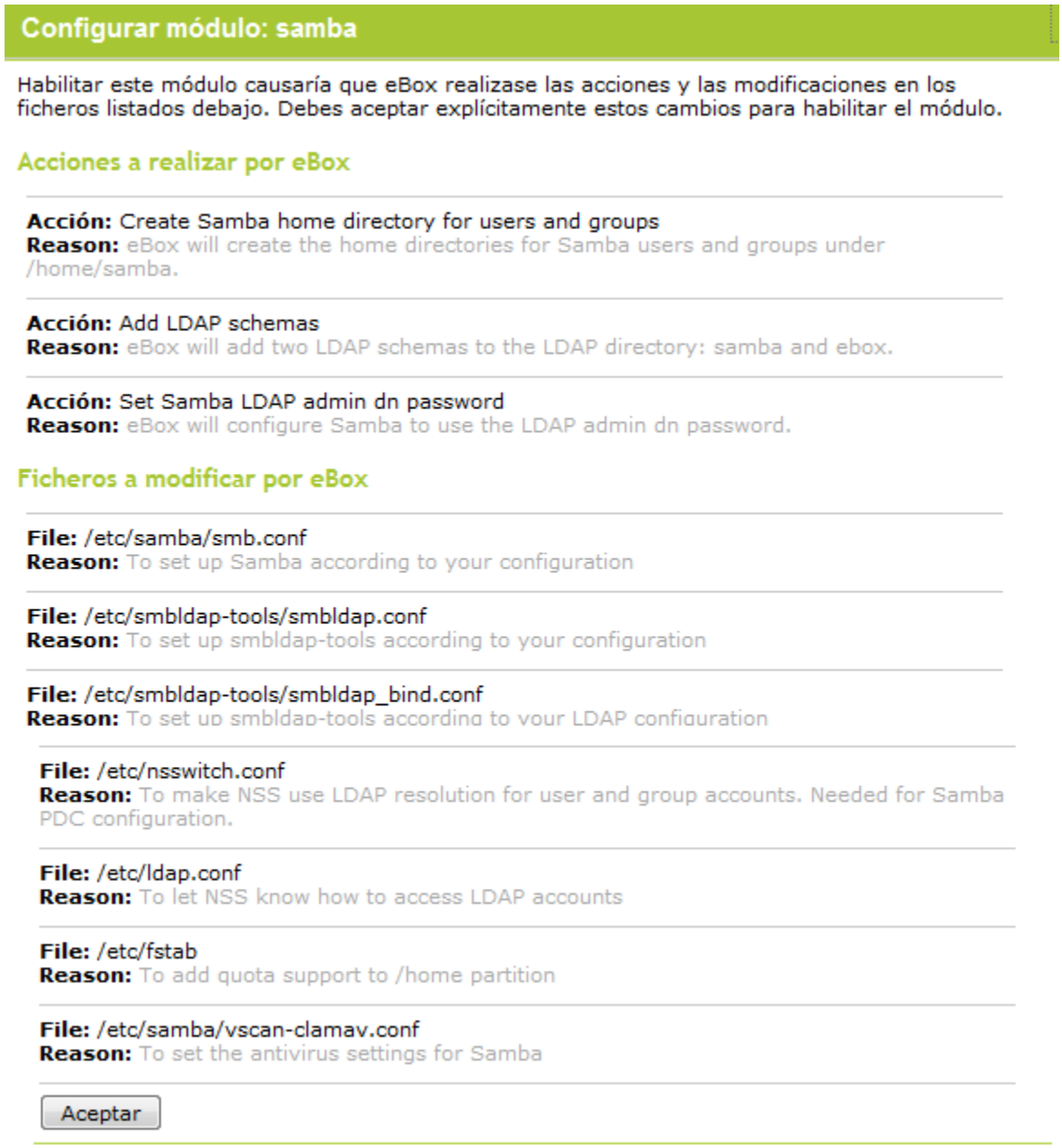


Figura 22. Formulario Emergente al Activar el Módulo Compartir Ficheros

Figura 23. Formulario Emergente al Activar el Módulo Compartir Impresoras

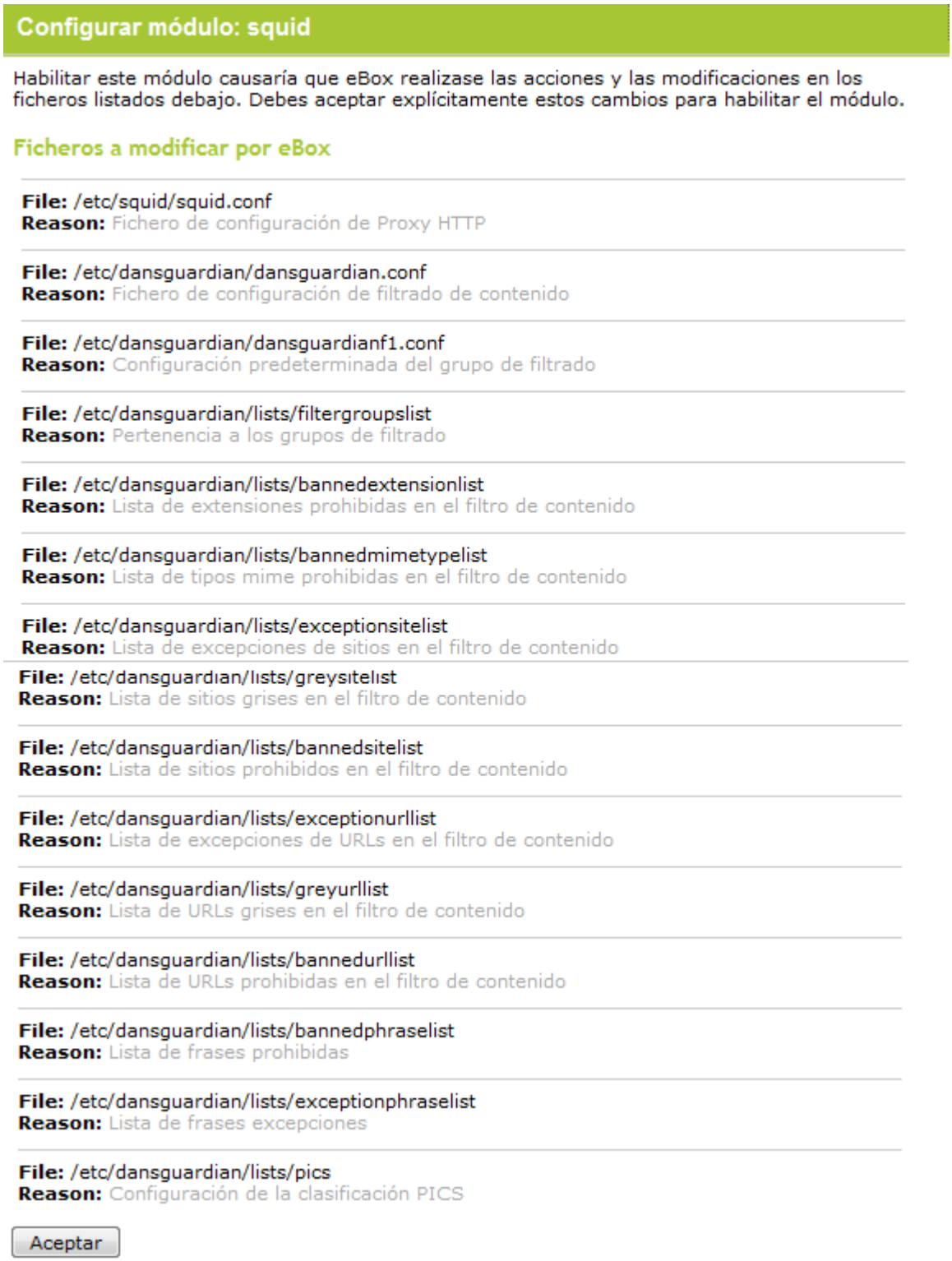


Figura 24. Formulario Emergente al Activar el Módulo Proxy HTTP

Ahora ya están activos cada uno de los módulos y lo que resta forma parte de la configuración.

Figura 25. Estado de los Módulos después de la activación

Todas estas autoconfiguraciones son las que hacen fácil el administrar el servidor. Debido a que no es necesario editar los archivos de configuración del sistema para poder lograr los resultados requeridos. Esto hace que la configuración sea una tarea sencilla de hacer.

5.2.2 CONFIGURACION DE EBOX OFFICE

La configuración de este modulo tiene por objeto activar el manejo de recursos y archivos compartidos en la red de Windows. Para cumplir con esta función, eBox hace uso del servicio de directorios OpenLDAP para el manejo de usuarios y de SAMBA para la compartición de archivos. Estos serán los dos recursos que se habilitaran en el servidor.

A continuación se explica cómo crear usuarios y grupos de usuarios en eBox. Sin embargo uno de los objetivos específicos de esta monografía consiste en evitar la creación de todos los usuarios uno a uno y en lugar de ello hacerlo de forma automática, aprovechando que en la organización existe un servidor Windows que tiene configurado el Directorio Activo y tiene creados a todos los usuarios de la organización VITELSA S.A. (Ver numeral 5.2.2.2)

5.2.2.1 Creación de Usuarios y Grupos

Habiendo ya activado los módulos de Usuarios y grupos y Compartir Ficheros. Es posible iniciar la creación de los usuarios existentes dentro de la organización en el servidor.

Para ello se seguirá la norma de creación según el estándar de la empresa y se agruparan según los departamentos que conforman.

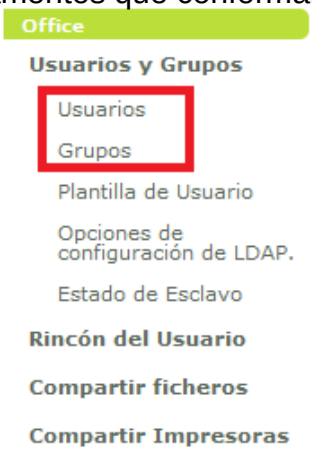


Figura 26. Menú de Configuración del Modulo Office

Creación de Usuarios:

Dar Click sobre **Usuarios**. Al hacer esto se mostrara en la zona central los campos que se deben diligenciar para ir creando los usuarios.

Nombre de Usuario: Nombre que el usuario utilizará para autenticarse en el dominio.

Nombre: Nombre del Usuario

Apellido: Apellido del Usuario

Comentario: Descripción detallada o más específica del usuario

Contraseña: Clave asignada al usuario para su autentificación.

Confirme Contraseña: Campo de verificación de la contraseña

Grupo: Nombre del Grupo al que pertenece el usuario. Este Campo puede dejarse en blanco cuando aun no se han creado los grupos correspondientes

Figura 27. Interfaz para Creación de Usuarios

Para la creación de un usuario simplemente se debe diligenciar los campos arriba mencionados y dar click sobre el botón 

En la figura puede verse dos usuarios ya creados: admsistemas y revisora. Una vez se han creado los usuarios es posible realizar cambios en la configuración.

Para realizar estos cambios se debe dar click en el botón  que se encuentra bajo la columna 

en la fila correspondiente al registro del usuario que se quiera modificar. Es posible modificar cualquier campo excepto el nombre de usuario asignado.

Al editar un usuario es posible:

• Crear una cuenta para compartir archivos o de PDC (Controlador de Dominio Primario) con una cuota personalizada.

• Asignar o Modificar el grupo al que pertenece el usuario.

• Asignar privilegios de Administrador.

• Dar permisos al usuario para usar una impresora.

• Crear una cuenta de correo electrónico para el usuario y un alias para la misma. (Valido en el caso de configurar el servicio de correo electrónico)

• Eliminar un Usuario.

Creación de Grupos:

Al igual que la creación de un usuario, para crear un grupo se deben diligenciar los campos correspondientes a la información requerida. De igual manera es posible editarlos una vez creados.

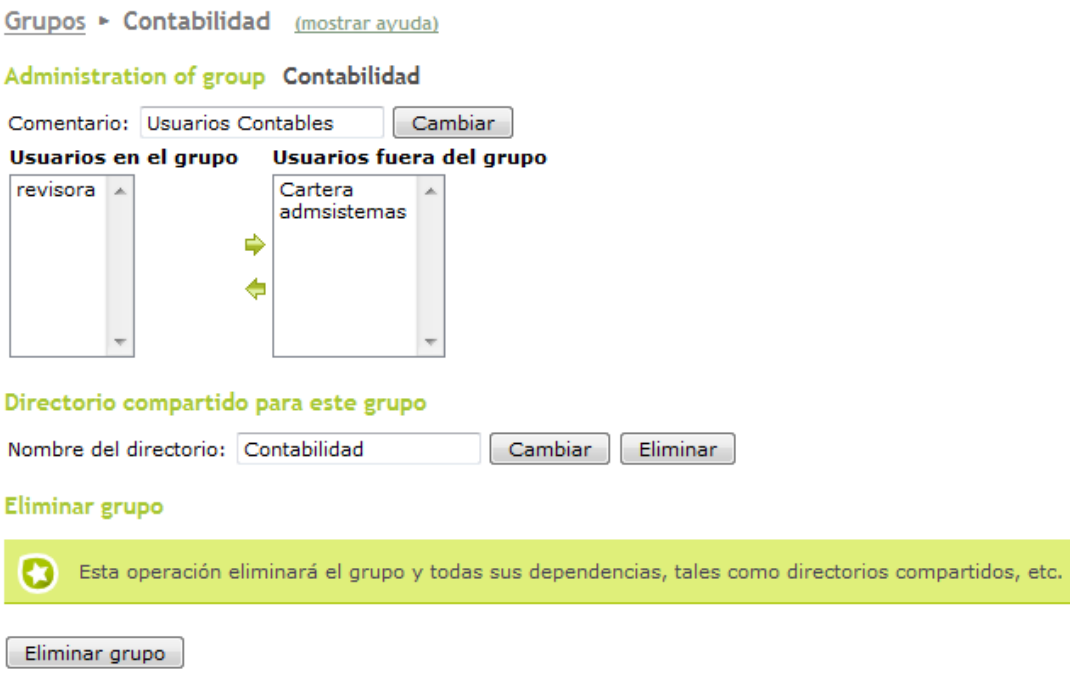
Al editar un grupo es posible:

• Cambiar la descripción del Grupo.

• Cambiar o incluir nuevos miembros al Grupo.

• Crear un directorio o carpeta compartida para los miembros del grupo.

• Eliminar un grupo.



Tareas a Seguir

Se deben crear algunos de los diferentes Grupos a los cuales pertenecerán los usuarios de la empresa. Estos Grupos son:

- Servicio Cliente
- Logística
- Gestión Pedidos
- Contabilidad
- Cartera
- Facturación
- Compras
- Calidad
- Sistemas

Para ello:

1. Ingresar al Modulo de *Office - Usuarios y Grupos – Grupos*. Crear el grupo **ServicioCliente** y dar click en el botón añadir para aceptar. El parámetro de comentario es opcional.

2. Continuar creando todo el listado de grupos. Al finalizar quedará el listado como se muestra a continuación:

Figura 28. Listado de usuarios creados

5.2.2.2 Sincronización de Zentyal con el Directorio Activo de Windows

En la sección anterior se vio como es posible ir creando los diferentes usuarios de la red y los grupos a los cuales pertenecen. Sin embargo existe la posibilidad de sincronizar los usuarios ya creados en el Directorio activo de Windows con el servidor de Zentyal (eBox). Este beneficio aplica para redes que trabajen bajo un dominio de Windows y quieran ser migradas a la plataforma Zentyal, facilitando el trabajo del administrador de la red, dado que es posible llevar automáticamente los usuarios ya creados dentro del dominio de la organización al nuevo servidor.

Para ello se deben tener en cuenta las siguientes consideraciones:

En el servidor Windows o controlador de dominio:

Descargar y ejecutar el instalador de *zentyal-adsync.exe*. Este aplicativo se puede descargar de la página de internet:

http://sourceforge.net/projects/zentyal/files/zentyal-adsync-2.0.1.exe/download

Al ejecutar el instalador se muestran las siguientes pantallas:

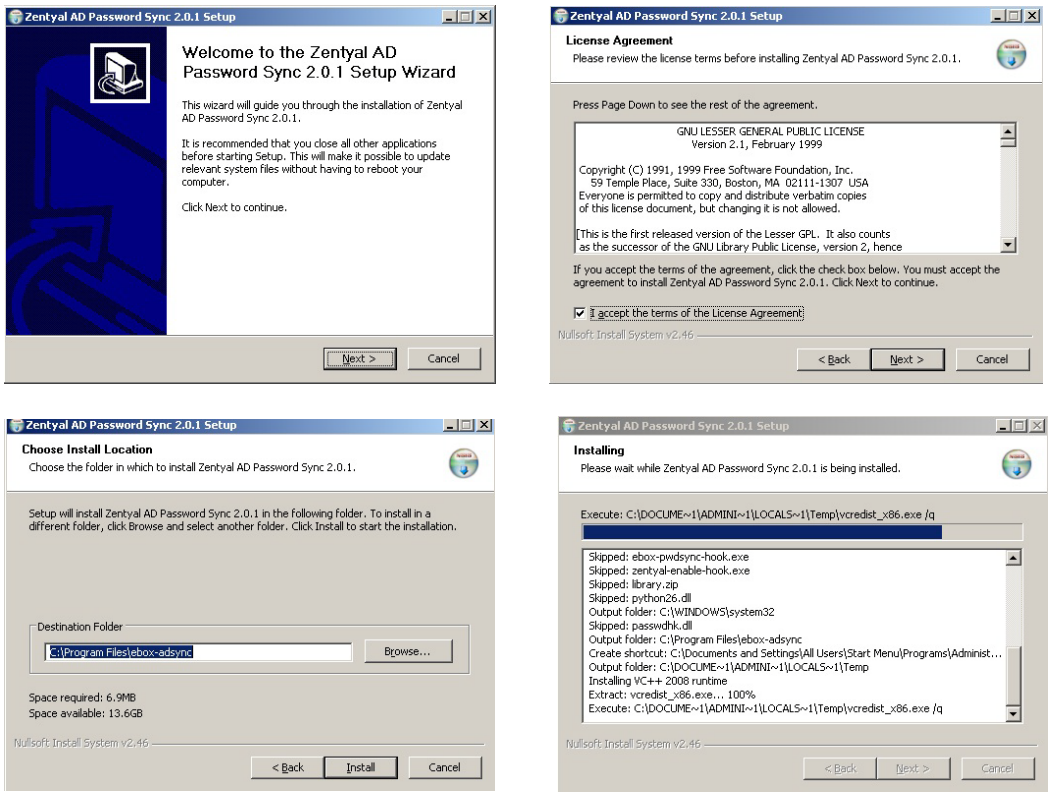
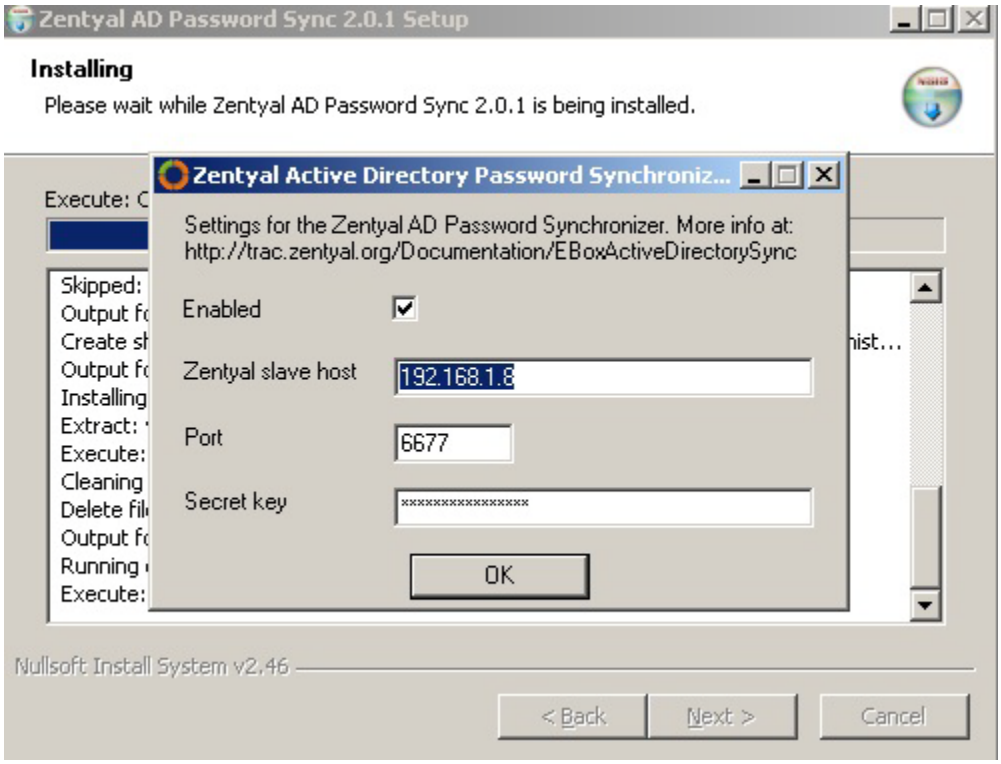


Figura 29. Imágenes del instalador de sincronizacion para el servidor windows



Al llegar a este punto se debe configurar los datos correspondientes a cada una de las casillas y explico los valores a continuación:

La casilla de verificación **Enabled** debe ser marcada para activar los cambios en el registro de Windows. Una vez se reinicie el servidor, esta aplicación será cargada automáticamente e iniciara el proceso de sincronización con la maquina Zentyal (Ebox)

En el campo **Zentyal Slave Host** se debe escribir la dirección IP de la maquina Zentyal.

El campo **Port** se propone el número de puerto 6677 para ejecutar este servicio, sin embargo se podría colocar otro número de puerto si así se quisiese. Teniendo en cuenta que posteriormente deberá configurarlo en la maquina Zentyal de igual manera.

El Campo **Secret Key** corresponde a una contraseña de 16 caracteres (alfanuméricos). Esta contraseña no debe tener caracteres especiales como: *, /,

&, #, etc. Dado que en la sincronización, el servicio no es capaz de interpretar estos caracteres y no es posible realizarse la sincronización.

Las políticas de Grupo en el servidor Windows deben tener activada la complejidad de las contraseñas. En una instalación típica de Windows server 2003 viene por defecto esta política, sin embargo debe verificarse. Para ello ir por **Administrative Tools→Domain Security Policy** y activar la complejidad de contraseñas si estas no se encuentras activadas (Ver imagen)

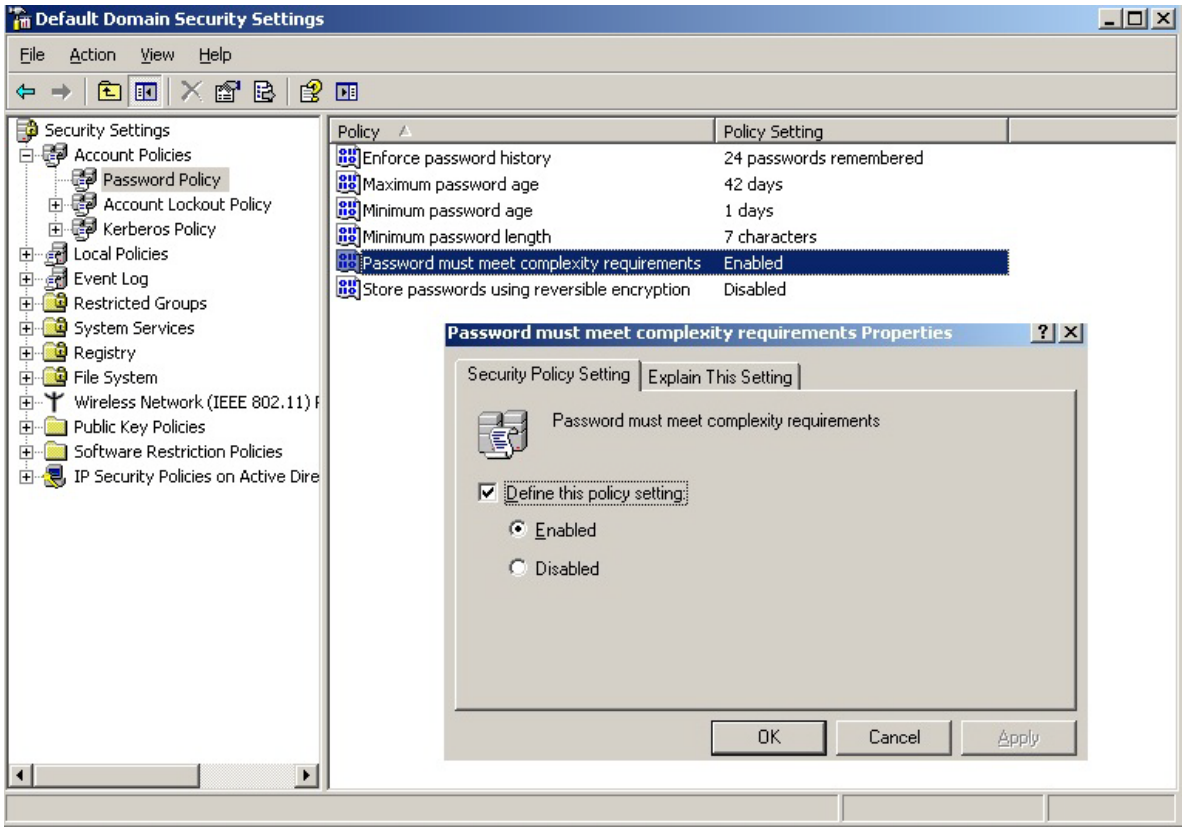
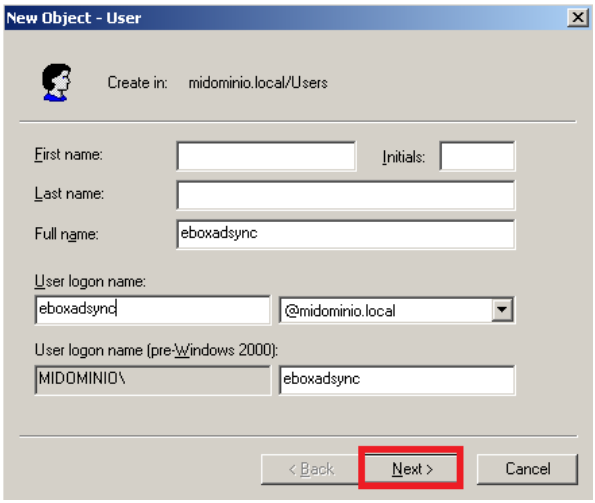


Figura 30. Definicion de Politica de seguridad para contraseñas en Windows

Adicional a esto debe crear un usuario que será utilizado por el protocolo LDAP para realizar la sincronización. Para ello se debe crear el Nuevo usuario en el directorio activo. Se recomienda dejar en blanco los campos Nombre (Name) y

apellido (Last Name) y escribir el mismo valor en los campos Nombre completo (Full Name) y Nombre de usuario inicio de sesión (User Logon Name)



Finalizar y reiniciar el servidor de Windows

En el servidor Zentyal (Ebox):

***NOTA**: No se debe configurar el modulo usuarios y grupos antes de realizar las siguientes parametrizaciones en el servidor Zentyal (Ebox).* Esto es fundamental.

- Ir a **Usuarios**- **Modo** completando los datos con la siguiente información:
  En **Modo**: Se debe seleccionar Windows AD Esclavo (Windows AD Slave)
  En **Master Host**: se escribirá la dirección IP del servidor de Windows que actúa como controlador de dominio (192.168.1.10)

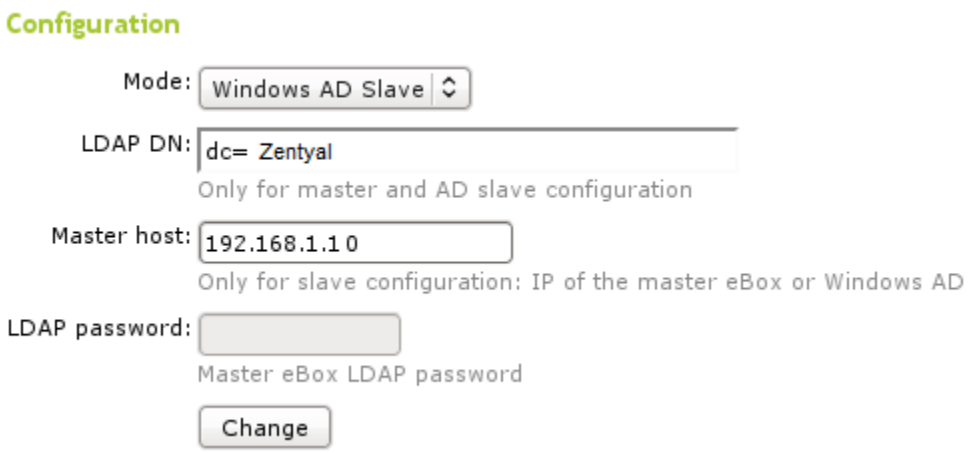
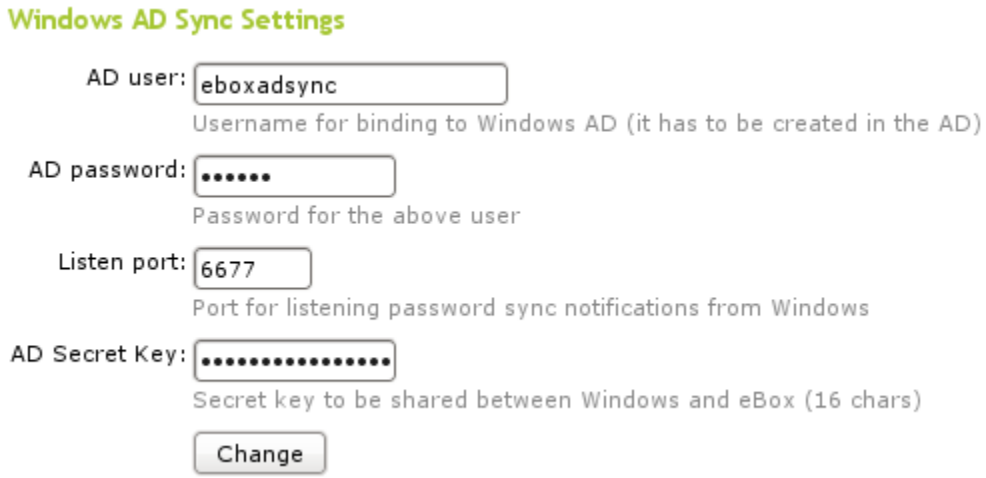


Figura 31. Configuración para sincronizacion con el Directorio Activo de Windows desde Zentyal

Después de estas dos configuraciones se deben guardar los cambios y posteriormente ya es posible activar el Modulo de Usuarios y grupos en la configuración del Estado del Modulo.

Ahora: ir a la sección **Usuarios y Grupos→AD Sync Settings** y completar la información solicitada



- **AD User**: Es el nombre de usuario que se crea en el directorio activo de Windows para realizar la sincronización. En este caso se creó la cuenta

eboxadsync pero puede dársele otro nombre. **AD password**: Es la contraseña de la cuenta de usuario anterior.

- **Listen Port**: Es el Puerto usado por el aplicativo que se instala en el servidor de Windows. Por defecto se propone el 6677 pero si se elige utilizar otro puerto, deberá colocar en este campo el puerto correspondiente para la sincronización.
- **AD Secret Key**: Es la contraseña de 16 caracteres que se digito cuando se instalo la aplicación en el servidor Windows Server. Es imprescindible que sea de 16 caracteres alfanuméricos, no se deben utilizar caracteres especiales como: * , /, # etc. Si se usan estos caracteres especiales, la sincronización puede no funcionar.

Al finalizar estas dos configuraciones tanto en el servidor Windows como en el servidor Zentyal (eBox), es necesario reiniciar las maquinas para que ocurra la sincronización. Para el caso de Vitelsa, fue necesario realizar más de una vez el procedimiento desinstalando y volviendo a instalar el aplicativo del servidor Windows ya que no se sincronizaba. El problema radicaba en las contraseñas pues inicialmente se habían usado caracteres especiales y no funcionaba. Al detectar esto se corrigió y se logro obtener la sincronización.

A continuación se muestra el listado de usuarios que se crearon automáticamente:

Name	Full name	Edit
Calidad01	Javier Amaya	
accesorios	Heriberto Meneses	
auxcalidad	Silvia Luna	
auxcartera	Olinda Sanchez	
auxcompras	Nelly Herrera	
auxfinanzas	Nury Vargas	
calidad02	Alex Luna	
cartera	Helena Monsalve	
cartera02	Maria Santos	
comercial01	Alix Rodriguez	

10 Page 1 of 4

Name	Full name	Edit
comercial02	Lilia Suarez	
comercial03	Eliana Contreras	
comercio_e	Nepo Hernandez	
contador	Nancy Castro	
diana.r	Diana Reivera	
eboxadsync	eboxadsync	
eboxadsynce	Sincronizacion	
facturacion	Beatriz Martinez	
finanzas	Jacqueline Cobos	
gerencia	Fernando Luna	

10 Page 2 of 4

Name	Full name	Edit
logistica01	Ligia Gomez	
logistica02	Dorian Sarmiento	
maria.p	Maria Portillo	
mesacorte	planta	
payulitas	Paula Sanchez	
practicante	Camila Perez	
practicante_ce	Leidy Penaranda	
produccion01	Yelitza Meneses	
produccion02	Sergio Meneses	
produccion03	Elkin Baez	

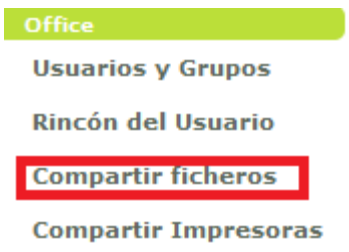
10 Page 3 of 4

Name	Full name	Edit
produccion04	Diego Rodriguez	
revisora	Sonia Melendez	
sistemas	Paula Sanchez	
soporte_ext	Jairo Villamizar	
subgerencia	Laura Luna	
subgerente	Freddy Luna	

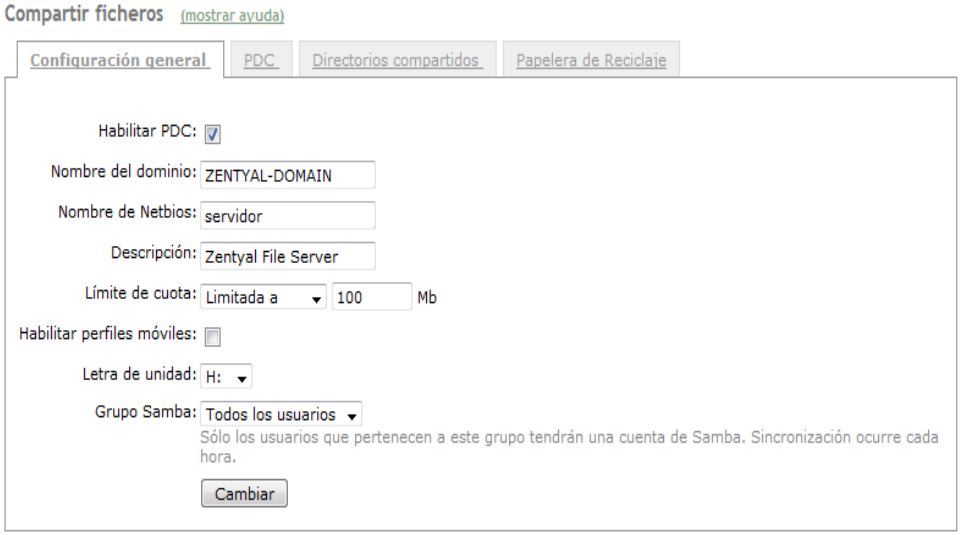
10 Page 4 of 4

5.2.2.3 Compartir Archivos

Como se menciono en la teoría del capítulo 4 para compartir archivos en un entorno Windows, Linux hace uso de SAMBA y para configurar esta utilidad dentro de eBox, se debe ingresar por el Modulo *Office-Compartir Ficheros*. En general es posible que cada usuario tenga su propia carpeta personal y adicional, cada grupo puede tener su carpeta compartida para todos los integrantes del grupo.



Al dar click en *Compartir Ficheros* se muestra entonces el formulario de configuración, donde es posible especificar diferentes parámetros:



El primero de ellos es la ***Configuración General***, donde se deben diligenciar ciertos campos que se explican a continuación:

Habilitar PDC: PDC es un sistema que permite el acceso restringido a un grupo de recursos donde con la combinación de un nombre de usuario y contraseña es posible acceder a ellos. Samba hace uso de este sistema de autenticación. Si queremos compartir archivos en un entorno de red, se debe habilitar esta opción.

Nombre de Dominio: Es el nombre del dominio donde trabajara la red de Windows.

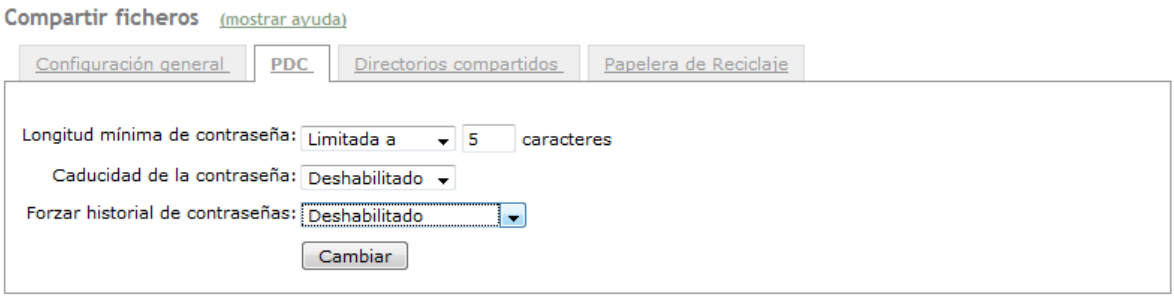
Nombre de Netbios: Es el nombre que identificará la maquina eBox dentro de la red de Windows.

Descripción: Es la descripción que se quiera hacer acerca del dominio

Límite de Cuota: Es posible establecer un límite máximo para la capacidad de las carpetas compartidas. O también se puede dejar deshabilitado. La selección de una u otra opción depende de la cantidad de espacio físico con el que se cuenta en el servidor.

Letra de Unidad y Grupo Samba: Es posible asignarle a un solo grupo de los usuarios creados una carpeta compartida en común para todos. La información contenida en dicha carpeta se puede compartir en los equipos clientes asignando la conexión a la unidad de red definida según la letra.

La segunda Pestaña corresponde al parámetro de configuración ***PDC*** *(Controlador de Dominio Primario)*

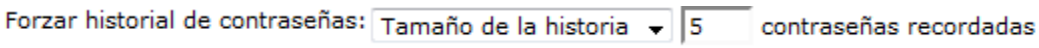


En este formulario se puede definir si se quiere manejar una **longitud mínima** para las contraseñas de los usuarios limitada a un cierto número de caracteres o si por el contrario se desea deshabilitar esa opción.

Caducidad para la Contraseña: Es posible establecer un número de días como plazo para vencerse las contraseñas. Por ejemplo se podría fijar un límite de 90 días para caducar. Pasado ese tiempo el usuario puede conectarse al servidor y cambiar el mismo su contraseña.

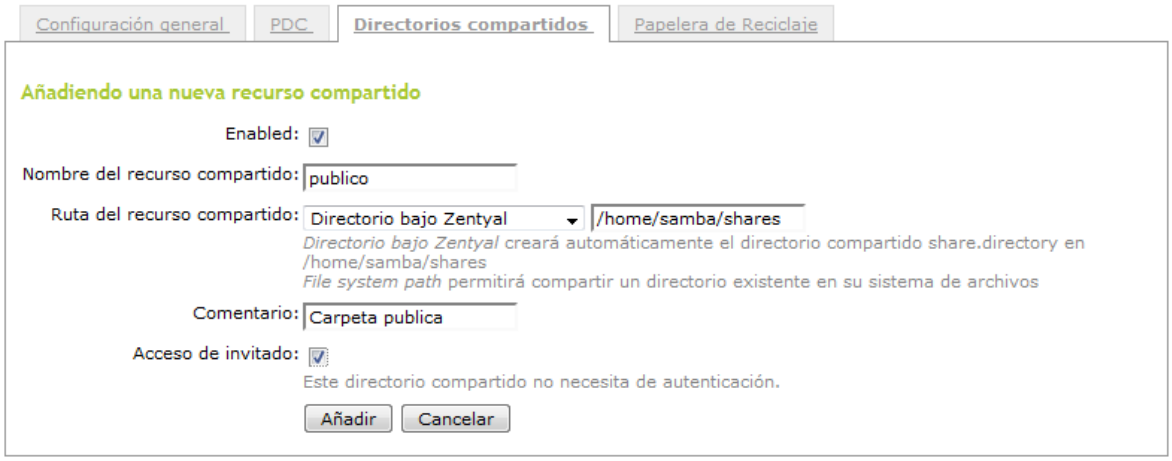
Forzar Historial de Contraseñas: El sistema puede configurarse para recordar un número de contraseñas establecidas. Si el usuario desea colocar la misma

contraseña, solo podría hacerlo pasado el tiempo fijado en este parámetro: Por ejemplo si el valor que coloco es 5, entonces solo hasta después de haber cambiado la contraseña 5 veces, es posible repetir alguna de las contraseñas ya usadas.



La tercera pestaña corresponde a ***Directorios Compartidos***, en esta sección es posible añadir las carpetas que se quieren compartir para todos los usuarios.

Para crear las carpetas, se debe hacer click en la opción Añade nuevo y automáticamente se mostrara en pantalla una serie de parámetros que deberán diligenciarse para cumplir con el propósito.



Donde:

Nombre del Recurso Compartido: Es el nombre de la carpeta que se quiere compartir.

Ruta del recurso compartido: Para el ejemplo se asigno la ruta /home/samba/shares, esto por razones de permisos, debido a que todo lo que esté por debajo de home es no restringido a los usuarios.

Comentario: El comentario que se quiere que aparezca a los usuarios de red.

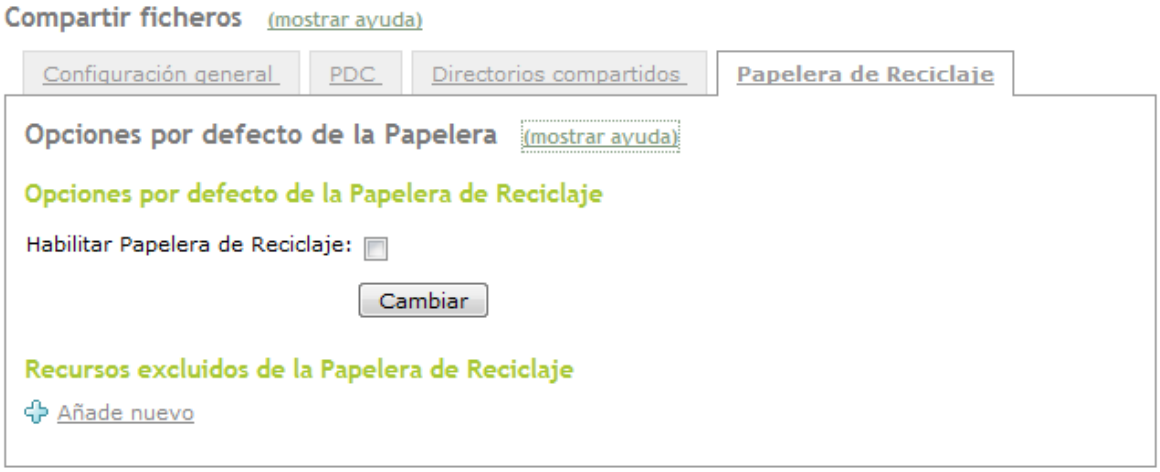
Acceso de Invitado: Al activar esta casilla es posible evitar la autenticación al intentar acceder a la carpeta.

Habiendo diligenciado esta información, se va armando la lista de carpetas compartidas

Desde esta lista, es posible editar el control de acceso. Es decir es posible asignar permisos de lectura, escritura o administración a un único usuario o a un grupo de usuarios. Los privilegios de administrador se dan sobre cualquier archivo contenido dentro de la carpeta sin importar cual usuario la haya creado.

Aunque como se vio con anterioridad, también es posible crear carpetas compartidas para los grupos desde la opción. *Usuarios y Grupos - Grupos*

Por último la cuarta pestaña corresponde a la **Papelera de Reciclaje**



Si nosotros activamos la papelera de reciclaje, la información borrada de las carpetas compartidas se envía a este sitio, en lugar de ser borrada definitivamente.

5.2.3 CONFIGURACION DE EBOX GATEWAY

La configuración de este modulo tiene por objeto principal activar la funcionalidad de el servicio de Proxy HTTP. Como se menciono anteriormente un proxy es un programa que actúa de intermediario en la conexión a un protocolo, que en el caso particular es HTTP. Al hacer la intervención puede modificar los datos recibidos y el comportamiento que van a tener esos datos.

Cuando tenemos este servicio en funcionamiento, es posible aplicar políticas de navegación para los usuarios de la red local. Por ejemplo establecer un Horario de navegación dentro de la red local, bloquear contenido no permitido según las políticas de la empresa, hacer selectividad entre las interfaces de red que pueden tener acceso a la WEB, etc. Squid va a ser el encargado de ayudarnos con el control de contenidos.

Adicional a ello se conformara una red más organizada y menos abierta a vulnerabilidades por acceso a información de fuentes ajenas de la organización.

5.2.3.1 Gestión de los Objetos de Red

Como se vio en la parte teórica, es posible definir objetos de red que posteriormente facilitaran la tarea de creación de reglas y aplicación de políticas para la navegación de internet.

Es necesario definir los objetos para los cuales se va a crear las reglas. Básicamente dentro de la organización se desean manejar dos objetos: Objeto 1: Corresponde a los miembro de la red, que son los equipos de todos los departamentos y los periféricos que están instalados. Objeto2: Corresponde a los equipos móviles que llegan esporádicamente a la organización y que pueden llegar a utilizar el recurso de internet pero no debe tener acceso a la información compartida dentro de la empresa.

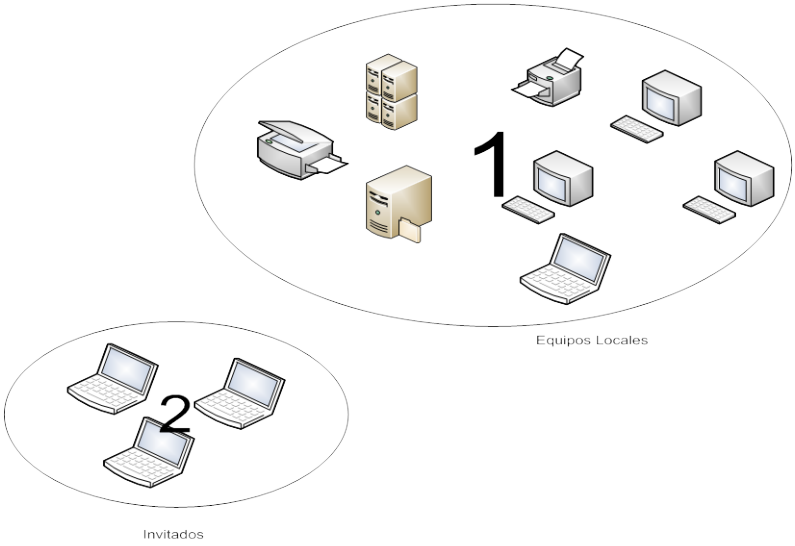


Figura 32. Definición de Objetos para VITELSA SA

Para ello se propone crear una red para los equipos de la organización y otra red que se asigne a los invitados. El servidor dispondrá del hardware de red necesario para tal configuración.

Para la definición de los objetos de red se debe ingresar por la sección Objetos del menú lateral izquierdo. Posteriormente se deben definir los nombres de los objetos e ir añadiéndolos a la lista. Para nuestro caso por ahora solo se crearan los objetos Invitados y Red Local. Después se debe dar click en el botón Guardar cambios que estará de color rojo en señal de que algo ha cambiado.

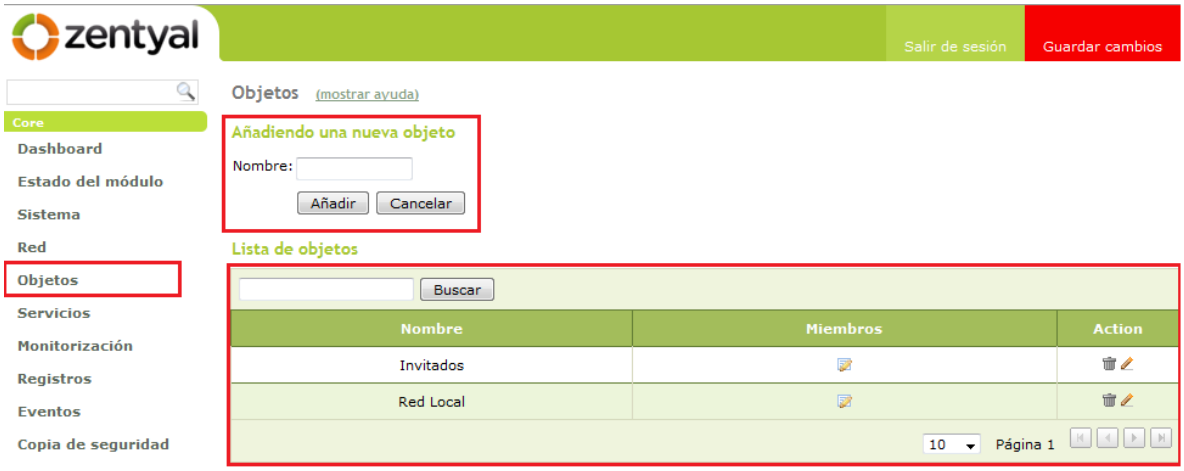


Figura 33. Creacion de los Objetos para la red de Vitelsa S.A

Una vez se han creado los objetos, el siguiente paso es asignar los miembros que lo conforman. Un objeto puede ser un dispositivo, un grupo de dispositivos o una red a la cual pertenezcan un grupo de dispositivos.

Los miembros de ambos objetos estarán definidos por las redes a las cuales pertenecen:

5.2.3.2 Configuración del Enrutamiento y Balanceo de Carga

La puerta de Enlace o Gateway es el router para los destinos que no se encuentran en la red local. Zentyal permite configurar en su servidor más de una puerta de enlace con el fin de distribuir el tráfico a través de dos conexiones diferentes.

Para la empresa el tener siempre activa su conexión a internet es un tema primordial. Por ello poseen dos alternativas diferentes de proveedores de internet. Sin embargo presentan inconvenientes debido al manejo que se le da a la segunda opción de internet puesto que es subutilizada. Su red actual siempre está conectada con el proveedor X. Cuando el servicio que presta X se cae, el profesional de sistemas debe movilizarse y adecuar la conexión con el proveedor Y. Esta solución no es la más adecuada pero es la que hasta ahora han manejado.

El siguiente diseño muestra una misma red compartida con los usuarios invitados que esporádicamente pueden llegar a la organización y que podrían llegar a vulnerar la información que se encuentra compartida en la red. Con la implementación de Zentyal como servidor dentro de la red se busca obtener una

solución a esta vulnerabilidad y aprovechar el balanceo de cargas que puede ser configurado para mejorar el ancho de banda uniendo los dos proveedores y garantizando trasparencia para los usuarios al momento en que alguno de los dos módems falle.

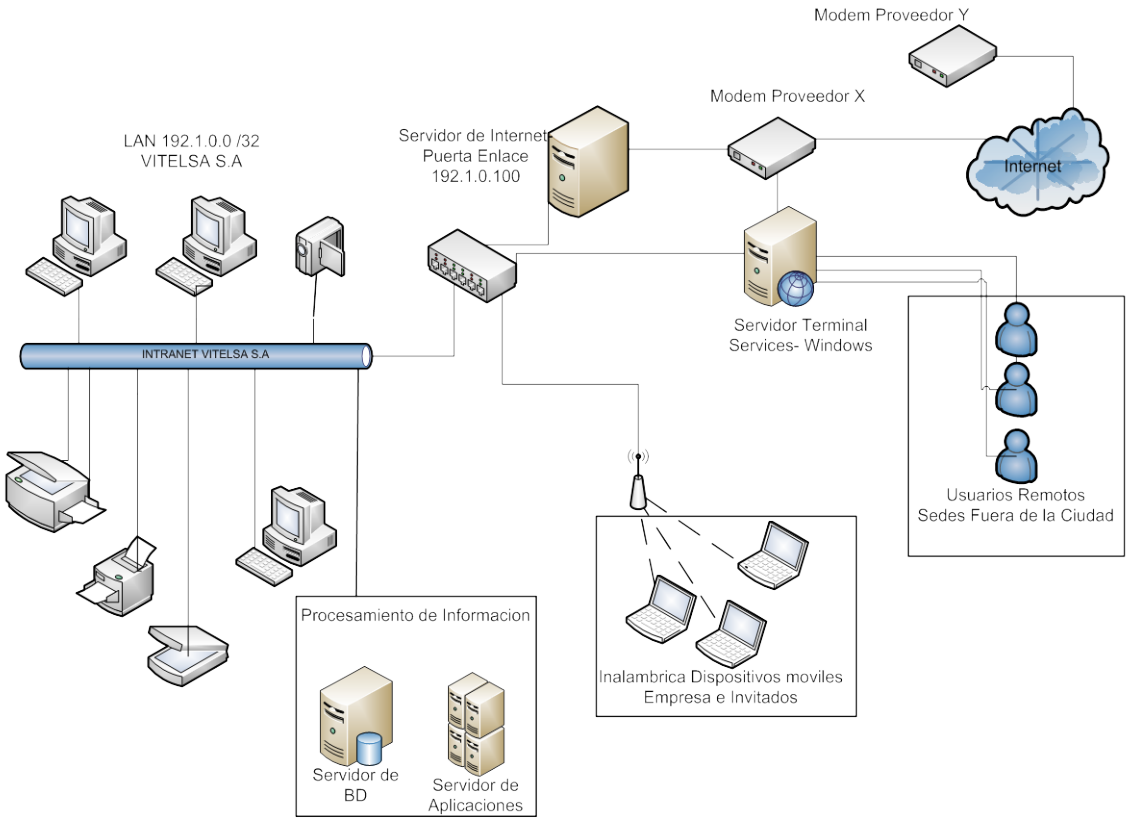


Figura 34. Diseño de Red Actual VITELSA S.A

Para cambiar el anterior diseño de red a modo que se pueda activar el uso de los dos proveedores de internet de forma simultánea y balancear el ancho de banda para cubrir los requerimientos se debe tener en cuenta que ninguna interfaz de red puede configurarse con DHCP debido a que se va a tener dos puertas de enlace

configuradas en el servidor, a las cuales se les asignara un peso especifico para priorizar la salida de datos por dichas interfaces.

Configuración de las puertas de Enlace:

Primero se deben configurar las dos puertas de enlace. Para ello previamente se ha definido cuales van a ser las dos subredes que se van a manejar dentro de la organización y se ha establecido sus respectivos Gateway.

Figura 35. Configuracion de Puertas de enlace- Balanceo de Cargas

Cada una de estas interfaces va a tener un peso que está acorde al ancho de banda que suministran dando prioridad a la de mayor peso. Esto quiere decir que de un total de 15 paquetes que se transmitan 10 irán por la interface eth0 y 5 por la interface eth1.

Posteriormente se debe ir por Red- Balanceo de Trafico y crear las reglas para las múltiples puertas de enlace.

Al balancear el tráfico estamos utilizando el 100% del ancho de banda que nos suministran nuestras conexiones ADSL. Sin embargo algo muy útil es configurar la tolerancia a fallos “WAN FailOver” para cuando alguna de las dos conexiones se caiga, con esto se evita la perdida de paquetes de datos dado que hemos configurado que una parte de los paquetes van por una puerta de enlace y la otra parte sale por la otra puerta de enlace.

Todo esto se basa en un conjunto de reglas para cada Gateway que necesariamente requiere comprobación. Entre estas reglas esta el hacer ping a una dirección de red, realizar una resolución de nombres de dominio o realizar una petición a un servidor web. Para ello la persona que configura las reglas establece un porcentaje de aceptación para las pruebas y si alguna de estas pruebas falla y no cumple el porcentaje de aceptación, automáticamente la interface es desactivada (puerta de enlace). Estas pruebas son cíclicas y por ende una vez se ha desactivado la interface y en la siguiente prueba se da un resultado exitoso, entonces nuevamente quedara activado sin que los usuarios de la red detecten el problema. Cuando las puertas de enlace definidas están operativas simultáneamente, el balanceo de cargas vuelve a operar según las reglas.

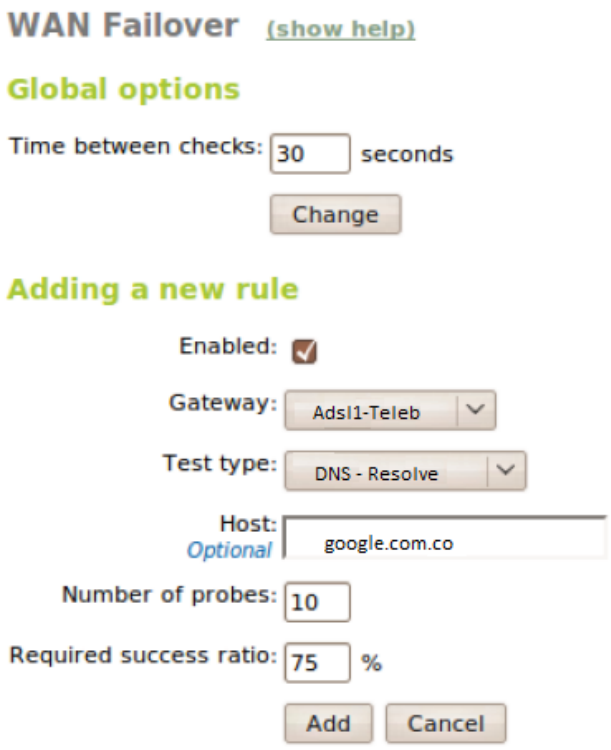
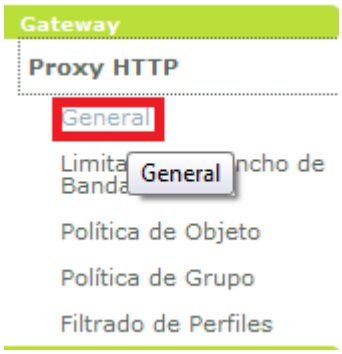


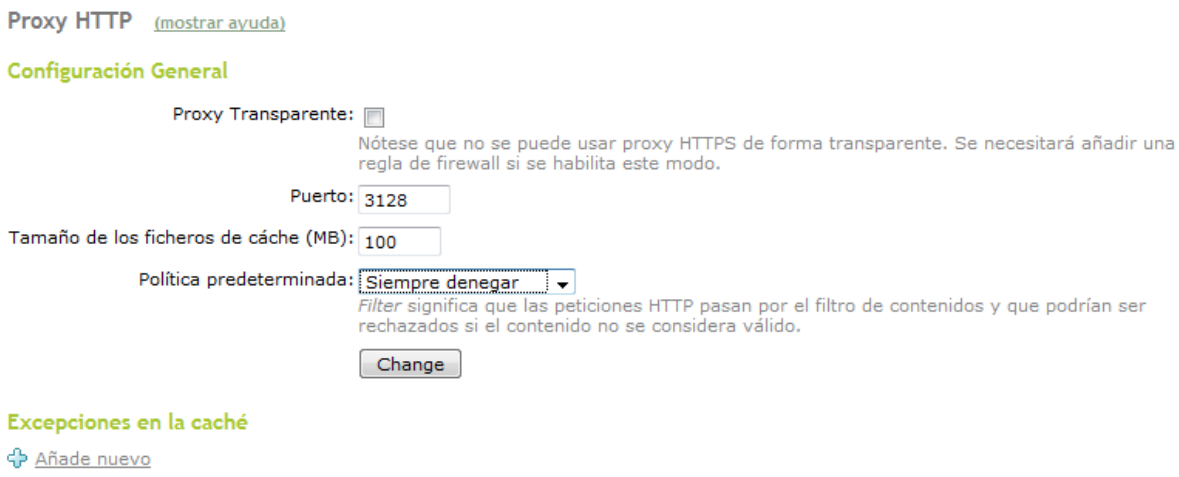
Figura 36. Configuración del WAN FailOver- Seguridad Balanceo de Cargas

5.2.3.3 Servicio Proxy HTTP



Dentro del Modulo Gateway, se encuentra el servicio Proxy HTTP. Para iniciar la configuración, ingresamos al modulo y damos click en la primera opción denominada: ***General***

Al hacer esto, se muestra la siguiente información en el formulario central:



Donde la Configuración General corresponde a los siguientes parámetros:

Proxy Transparente: Para explicar que es un proxy transparente, primero recordemos que un proxy es un intermediario que actúa entre la aplicación del cliente y un protocolo. Esto conlleva a que debe ser configurado del lado del cliente en sus aplicaciones de forma manual, en este caso los navegadores de

internet. Pero por esa misma razón es posible evadir ese control si un usuario cambia la configuración de su navegador.

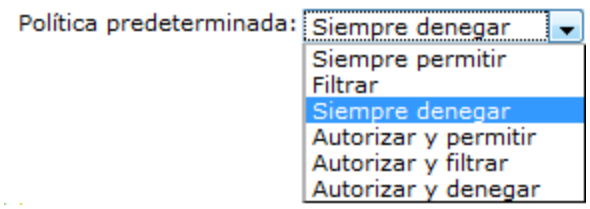
Un proxy transparente no requiere de la configuración del lado del cliente. Esa es la principal diferencia entre uno y otro. Es por esto que una manera de evitar el trabajo de configurar cada navegador de los usuarios en la red es usar el ***proxy transparente***. Para esto en la configuración de las interfaces de red de los clientes, debe quedar establecido nuestra dirección del equipo Zentyal como Gateway (Puerta de enlace), de ese modo las conexiones se redirigen al proxy. Sin embargo las conexiones seguras (HTTPS) no pueden ser filtradas pues están cifradas. Por lo cual hay que establecer una regla en el cortafuegos para garantizar el paso de este tipo de conexiones.

Para nuestro servidor, vamos a utilizar el proxy transparente. Porque no queremos usuarios que nos evadan la norma. Por tanto debemos marcar esta opción.

Puerto: El puerto por defecto es el 3128, pero se puede configurar a otro puerto. Otros puertos típicos para servicios de proxy web son el 8000 y el 8080.

Vamos a cambiar el puerto al 8080 en la configuración.

Lo primero a realizar es la configuración de una política de acceso global, para ello el sistema dispone de 6 políticas predefinidas y debemos seleccionar una de ellas.



Una de las políticas de la organización es dar acceso a solo las aplicaciones y links relativos a la operación de la empresa. Esto es: aplicaciones como correo electrónico, paginas de bancos con quienes se manejan las cuentas, paginas de proveedores de productos comercializados por la empresa y paginas relativas a las obligaciones financieras y tributarias. Es fácil optar por la política de denegar todo e ir filtrando las pocas páginas que están autorizadas por la organización.

CONCLUSIONES

Algunas veces el desarrollo o implementación de este tipo de proyectos que incluyen software libre no se da en las pequeñas y medianas empresas debido al miedo de los encargados de administrar los sistemas por el desconocimiento del software o porque no existen empresas que presten soporte en el mercado a estas plataformas. Sin embargo este mito queda de lado al usar Zentyal puesto que su diseño modular y la configuración automática a través de plantillas hace que para una persona con conocimientos mínimos en Linux sea posible ajustar nuevas funcionalidades dentro del mismo sin correr el riesgo de dañar alguno de los archivos de configuración.

La migración del directorio activo de Windows a la plataforma Zentyal, beneficia a la organización Vitelsa S.A en el marco de la legalidad de software frente a la Ley 603 de 2000.

Se subsanaron las vulnerabilidades relativas al acceso de información por parte de agentes externos de la organización puesto que Vitelsa S.A no tenia definida ninguna política de seguridad en cuanto a permisos a los usuarios temporales de la red. Cuando una persona ajena a la organización llegaba con algún dispositivo móvil y este se conectaba a la red, tenía la posibilidad de ver y acceder a todos los documentos compartidos que se encontraban en ella. Al separar la red interna de la red de invitados utilizando la definición de objetos de red y aplicando políticas de seguridad, esta vulnerabilidad queda subsanada.

Se logro el objetivo de sincronizar los usuarios del directorio activo de Windows con el servidor Zentyal facilitando la labor de crear todos los usuarios en un tiempo record y sin tener configurar manualmente cada uno de ellos.

Gracias al balanceo de cargas se dio un buen uso al servicio de internet contratado a través de sus dos proveedores. Se resolvieron problemas de forma y de operación en el momento de fallos por parte de uno de los dos ISP. Para la organización es transparente el manejo que se le da a estos fallos y el responsable de sistemas ya no tiene que preocuparse cuando se presenta esta situación.

BIBLIOGRAFIA

Caso de Éxito EBox Platform. Sevilla España. Configuración de una red única bajo está plataforma para ser usada por 21 oficinas del Organismo Provincial de Asistencia Económica y fiscal OPAEF. Disponible en internet: http://www.zentyal.com/wp-content/uploads/2010/07/OPAEF_eBox_caso_de_exito_es.pdf

Centro de excelencia de software libre de Castilla La Mancha. Análisis de la Aplicación EBox Platform. Año 2010. Disponible en internet en el sitio: http://www.ceslcam.com/analisis-de-aplicaciones/analisis-de-aplicacion-ebox-platform.html

Gustavo Pimentel. Blog acerca del desarrollo de EBox Platform 1.5-1. Documentación relacionada. Disponible en internet en el sitio: http://www.gustavopimentel.com.ar/2010/08/en-desarrollo-ebox-platform-1-5-1/

Contribuciones de usuarios al repositorio EBox. Sincronización de dos servidores Maestro- Esclavo haciendo uso del servicio de directorios LDAP. Disponible en internet: http://trac.ebox-platform.com/wiki/Document/HowTo/EBoxSeville_Spanish_Only

Documentación Pagina Oficial Zentyal Org: http://www.zentyal.com/es/

Documentación Contribuciones de usuarios al Foro de Zentyal Platform. Configuración del Directorio activo de Windows con un servidor Zentyal. Disponible en internet en el sitio: http://trac.zentyal.org/wiki/Document/Documentation/ActiveDirectorySync

COLOMBIA. CONGRESO DE LA REPUBLICA. Ley 603 de 2000 Por la cual se modifica el artículo 47 numeral 4 de la Ley 222 de 1995. Derechos de autor.