DISEÑO E IMPLEMENTACIÓN DE PROYECTOS CON SOFTWARE LIBRE BAJO SISTEMAS OPERATIVOS LINUX Y PLATAFORMA CON LICENCIA DE PAGO

CAMILO ANTONIO DUARTE MARTÍNEZ

FUNDACIÓN UNIVERSITARIA LOS LIBERTADORES
FACULTAD DE INGENIERÍA
INGENIERÍA DE SISTEMAS
BOGOTÁ
2015

DISEÑO E IMPLEMENTACIÓN DE PROYECTOS CON SOFTWARE LIBRE BAJO SISTEMAS OPERATIVOS LINUX Y PLATAFORMA CON LICENCIA DE PAGO

CAMILO ANTONIO DUARTE MARTÍNEZ

TRABAJO DE GRADO PARA OPTAR POR EL TÍTULO DE INGENIERO DE SISTEMAS

Director de tesis: INGENIERO AUGUSTO JOSE ANGEL MORENO

FUNDACIÓN UNIVERSITARIA LOS LIBERTADORES
FACULTAD DE INGENIERÍA
INGENIERÍA DE SISTEMAS
BOGOTÁ
2015

Nota de Aceptación

_____

_____

_____

_____

Presidente del Jurado

_____

Jurado

_____

Jurado

Bogotá, 04 de Junio de 2015

El presente proyecto va dedicado especialmente a mis padres y compañeros ya que gracias a la colaboración y empuje fue posible la realización de cada uno de los proyectos.

AGRADECIMIENTOS

Yo Camilo Antonio Duarte Martínez, doy cordialmente un agradecimiento a aquellas personas que con su voluntad de apoyo incondicionalmente ayudaron a que cada uno de los proyectos tuviera desarrollo triunfante, sobre todo a mis padres y compañeros que confiaron completamente en mí, los docentes que tuvieron un papel muy importante a la hora de asesorarme y brindar colaboración con todo lo que necesité.

TABLA DE CONTENIDO

TABLA DE ILUSTRACIONES

LISTA DE TABLAS

GLOSARIO

AGENTE: es un complemento desarrollado por el proveedor para que su aplicativo funcione a través de un túnel entre el servidor y el cliente el cual tenga el agente instalado.

BACKUP: es la copia total o parcial de información importante del disco duro, CD, bases de datos u otro medio de almacenamiento.[1]

DMZ: es un diseño conceptual de red donde los servidores de acceso público se colocan en un segmento separado, aislado de la red. La intención de DMZ es asegurar que los servidores de acceso público no puedan comunicarse con otros segmentos de la red interna, en el caso de que un servidor se encuentre comprometido.[2]

DOS: son las siglas de Distributed Denial of Service. La traducción es "ataque distribuido denegación de servicio "y traducido de nuevo significa que se ataca al servidor desde muchos ordenadores para que deje de funcionar.[3]

EMAL ENCRYTION: cifrado de correo electrónico administrado de forma centralizada para proteger las comunicaciones de correo electrónico.[4]

FILE SERVER: un tipo de servidor que almacena y distribuye diferentes tipos de archivos entre los clientes de una red de ordenadores. Su función es permitir a otros nodos el acceso remoto a los archivos que almacena o sobre los que tiene acceso.[5]

FIREWALL: los cortafuegos (firewall) pueden ser software, hardware, o una combinación de ambos. Se utilizan con frecuencia para evitar que los usuarios desautorizados de Internet tengan acceso a las redes privadas conectadas con Internet, especialmente intranets.[6]

LAN: una red de área local y permite la interconexión de uno o varios dispositivos.[7]

LOG: uno o más ficheros de texto automáticamente creados y administrados por un servidor, en donde se almacena toda la actividad que se hace sobre éste. Cada

1 http://www.alegsa.com.ar/Dic/backup.php

2 http://www.tp-link.es/article/?faqid=28

3 http://www.genbeta.com/web/son-los-ataques-ddos-efectivos-como-medio-de-protesta

4 http://www.symantec.com/es/mx/gateway-email-encryption/

5 http://es.wikipedia.org/wiki/Servidor_de_archivos

6 https://www.masadelante.com/faqs/cortafuegos

7 http://es.wikipedia.org/wiki/Red_de_computadoras

servidor, dependiendo de su implementación y/o configuración, podrá o no crear determinados log's.[8]

GPL: la Licencia Pública General de GNU o GPL por sus siglas en inglés, es una licencia creada por la Free Software Foundation, que está orientada principalmente a proteger la libre distribución, modificación y uso de software. Su propósito es declarar que el software cubierto por esta licencia es software libre y protegerlo de intentos de apropiación que restrinjan esas libertades a los usuarios.[9]

LOGANALYZER: servidor centralizado de Log's.[10]

MY-SQL es el servidor de bases de datos relacionales más popular, desarrollado y proporcionado por MySQL AB.[11]

OPENPGP: es un estándar de internet para la interoperabilidad de mensajes protegidos con criptografía.[12]

PHP: es un lenguaje de código abierto muy popular especialmente adecuado para el desarrollo web.[13]

PHISHING: es un tipo de engaño creado por hackers malintencionados, con el objetivo de obtener información importante como números de tarjetas de crédito, claves, datos de cuentas bancarias, etc. El objetivo más común, suele ser la obtención de dinero del usuario que cae en la trampa. Por lo general, el engaño se basa en la ignorancia del usuario al ingresar a un sitio que presume legal o auténtico.[14]

POP3: descarga los mensajes eliminándolos del servidor. Los mensajes de correo electrónico ya no se encuentran disponibles por correo web o un programa de correo.[15]

PORTAL CAUTIVO: es un programa o máquina de una red informática que vigila el tráfico HTTP y fuerza a los usuarios a pasar por una página especial si quieren navegar por Internet de forma normal.[16]

---

8 http://www.alegsa.com.ar/Dic/server%20log.php

9 https://www.isocron.net/node/36

10 http://linuxprience.blogspot.com/2012/08/6-servidor-centralizado-de-logs.html

11 indira-informatica.blogspot.com/2007/09/qu-es-mysql.html

12 http://www.alegsa.com.ar/Dic/openpgp.php

13 http://php.net/manual/es/intro-whatis.php

14 http://www.alegsa.com.ar/Dic/phishing.php

15 http://www.one.com/es/support/faq/que-significa-imap-y-pop3

16 http://es.wikipedia.org/wiki/Portal_cautivo

POSTFIX: es un servidor de correo de software libre / código abierto, un programa informático para el enrutamiento y envío de correo electrónico.[17]

POSTGRESQL: es un sistema de gestión de bases de datos objeto-relacional, distribuido bajo licencia BSD y con su código fuente disponible libremente.[18]

PROXY: un servidor proxy es un equipo que actúa de intermediario entre un explorador web (como Internet Explorer) e Internet. Los servidores proxy ayudan a mejorar el rendimiento en Internet ya que almacenan una copia de las páginas web más utilizadas.[19]

RELAY: permite que cualquier usuario de Internet lo use para enviar correo electrónico a través de él.[20]

RSYNC: es una aplicación libre para sistemas de tipo Unix y Microsoft Windows que ofrece transmisión eficiente de datos incrementales, que opera también con datos comprimidos y cifrados.[21]

S/MIME: es un protocolo que añade firmas digitales y encriptación a los mensajes MIME. MIME es el formato estándar propuesto para correo electrónico.[22]

SEGURIDAD: es un ordenador o máquina informática que está al "servicio" de otras máquinas, ordenadores o personas llamadas clientes y que le suministran a estos, todo tipo de información.[23]

SSH: es el nombre de un protocolo y del programa que lo implementa, y sirve para acceder a máquinas remotas a través de una red. Permite manejar por completo la computadora mediante un intérprete de comandos.[24]

SMTP: el acrónimo SMTP proviene de Simple Mail Transfer Protocol (Protocolo de Transferencia de Correo Simple), es decir, el procedimiento que permite el transporte del email en la Internet.[25]

SOPHOS UTM: es un software o appliance con características de firewall, proxy, WAF.

---

17 http://es.wikipedia.org/wiki/Postfix

18 http://www.postgresql.org.es/sobre_postgresql

19 http://windows.microsoft.com/es-co/windows-vista/what-is-a-proxy-server

20 http://es.wikipedia.org/wiki/Open_Relay

21 http://es.wikipedia.org/wiki/Rsync

22 http://ca.banesto.es/ayuda/faqs/mime2.html

23 http://aprenderaprogramar.com/index.php?option=com_content&view=article&id=542:que-es-un-servidor-y-cuales-son-los-principales-tipos-de-servidores-proxydns-webftppop3-y-smtp-dhcp&catid=57:herramientas-informaticas&Itemid=179

24 http://es.wikipedia.org/wiki/Secure_Shell

25 http://www.serversmtp.com/es/que-es-servidor-smtp

SSL: Secure Sockets Layer es un protocolo diseñado para permitir que las aplicaciones para transmitir información de ida y de manera segura hacia atrás.[26]

TERMINAL SERVICES: los Servicios de Escritorio Remoto, antiguamente conocido como Servicios de Terminal son un componente de los sistemas operativos Windows que permite a un usuario acceder a las aplicaciones y datos almacenados en otro ordenador mediante un acceso por red.[27]

WAF: un tipo de firewall que se utilizan para controlar el acceso a una aplicación o servicio web.[28]

ZIMBRA: es una suite de correo electrónico mensajería y colaboración innovadora.[29]

26 https://www.digicert.com/es/ssl.htm

27 http://es.wikipedia.org/wiki/Terminal_Services

28 http://www.welivesecurity.com/la-es/2013/12/20/web-application-firewall-como-proteger-su-aplicacion-web-con-modsecurity/

29 http://aprendiendozimbra.blogspot.com/2011/07/pantalla-principal.html

RESUMEN

En el desarrollo de cada uno de los proyectos se hizo levantamiento de información por parte del gerente de cuenta de la compañía en el cual los hallazgos encontrados fueron argumentados en una reunión que se tuvo entre las áreas comerciales e ingeniería para poder ejecutar cada uno de los proyectos.

Algunas implementaciones realizadas fueron basadas con software de código cerrado la cual cumplió con las necesidades del cliente y tienen los recursos económicos para adquirirla pero sin tener en cuenta el costo de la herramienta. Los proyectos ejecutados en cada una de las compañías son útiles para generar mejoras tanto para la red como para los usuarios quienes hacen uso de ellas contribuyendo a la mejor satisfacción y eficiencia de las actividades diarias con la ayuda de herramientas colaborativas pero siempre primando que los usuarios a los cuales se les ofrece el servicio sean más efectivos y productivos con las labores asignadas y dependiendo de su rol en la compañía estableciendo una serie de políticas necesarias para cumplir con dicho objetivo. A cada proyecto se le ofrecieron diferentes alternativas de solución pero ya sea por costos y/o confidencialidad de la información algunas de ellas las adquirieron para satisfacer las necesidades de la compañía ya sea porque en realidad es una necesidad o simplemente por cumplir con recomendación de auditorías internas o externas.

Además de todos los beneficios que otorgan las herramientas anteriormente descritas, se debe tener seguridad sobre la red y esto se hace sobre algunos proyectos en el cual se realiza la implementación de firewalls por software y por hardware para la protección perimetral y de aplicaciones para prevenir el ingreso no autorizado sobre la red LAN.

PALABRAS CLAVE:
Migración servidor, implementación, seguridad perimetral, aprendizaje, copias de seguridad, sistema operativo, open source, código libre.

1. INTRODUCCIÓN

Para que la infraestructura de red sea segura y funcione de manera efectiva, deben identificarse las posibles amenazas y/o debilidades, conocer y prever posibles incidentes. Por tanto, a través de este informe es dar a conocer proyectos los cuales están basados en situaciones reales de empresas que contaban con riesgo o que querían mejorar su sistema, estos proyectos brindan soluciones especializadas, desde la consultoría, gestión, captura de requisitos, análisis, validación, puesta en marcha, mantenimiento y/o soporte, esto basado en la necesidad de cada empresa y/o desarrollo de nuevas ideas, basadas en herramientas Open Source y/o licenciados a fin de reducir y/o eliminar las posibles fallas y mejorar el rendimiento de la empresa siempre de la mano con seguridad de la información y seguridad perimetral. A continuación se pasa a detallar algunos aspectos relativos al desarrollo de cada proyecto:

El primer proyecto se basa en la migración de una base de datos PostgreSQL e instalación de sistema operativo RedHat con arquitectura x64 Bits para el funcionamiento de la misma, el segundo proyecto es la instalación de un servidor Windows Server 2008 R2 con arquitectura x64 Bits, en el cual se realiza la instalación y configuración del aplicativo Acronis Backup & Recovery 11.5 Management Server y se desea tener una copia de seguridad de los servidores principales (Base de datos, Terminal Services, Active Directory, File Server y Servidor de aplicaciones), el tercer proyecto se enfoca en la migración de un servidor de correo Horde con 150 cuentas el cual estaba siendo ejecutado en un sistema operativo Fedora 15 con arquitectura x64 Bits dichas cuentas se desean migrar a un servidor de correo Zimbra Collaboration Suite versión 8 con Sistema operativo CentOS 6.5 de arquitectura x64 Bits, el cuarto proyecto es la instalación y configuración de un servidor de LOG'S para centralizar todos los registros de los dispositivos en la red y poder determinar la causa de alguna falla o el monitoreo de las aplicaciones, también se desea hacer la migración de un servidor firewall PfSense a un servidor SOPHOS UTM con licenciamiento fullguard (Network Security, Mail Security, Web Security, Web Application Security, Wireless Security) en el cual se deben crear y depurar reglas para el mejor funcionamiento. El quinto proyecto es la instalación y configuración de firewall pfSense con servicios de "Filtro de contenidos, protección de la red a nivel perimetral, conexión mediantes VPN".

2. OBJETIVOS

2.1 OBJETIVO GENERAL

Ejecutar proyectos para brindar solución a las necesidades de las empresas por medio de la implementación de herramientas colaborativas de software libre (OpenSource) y herramientas con subscripción, las cuales tienen la finalidad de mejorar el rendimiento y productividad laboral de las empresas.

2.2 OBJETIVOS ESPECÍFICOS

- Implementar herramientas OpenSource para la integración de recursos de red.
- Establecer niveles de seguridad y confiabilidad aceptables para el envío y recepción de datos entre diferentes redes.
- Implementar una herramienta para realizar copias de seguridad y mantener en custodia o de forma segura la información y así mismo mantener la continuidad del negocio.
- Definir esquemas de seguridad perimetral que involucren firewalls y sistemas de detección de intruso (IDS).
- Implementar web application firewalls (WAF), sistemas de prevención de intrusiones para aplicativos web.

3. JUSTIFICACIÓN

El principal activo o valor de una empresa, sin duda, es la información, objeto que se ha convertido en algo con un valor inmenso no solo para las empresas sino para todos los usuarios ya que cualquier incidente que repercuta sobre ésta va a suponer un perjuicio para la empresa.

Como es bien sabida una de las maneras más conocidas de usurpación, robo o saboteo de información son los ataques externos e internos hacia los servidores donde cada proceso es un registro almacenado local o remotamente. Para mantener la trazabilidad de las aplicaciones y así poder obtener la integridad, confidencialidad y disponibilidad de los procesos realizados, es necesario el uso de herramientas desarrolladas por comunidades sin ánimo de lucro o de código cerrado que traen como beneficio para la infraestructura de cada empresa confiabilidad y seguridad, ya que estas permitirán detectar y/o predecir situaciones de riesgo a través de herramientas colaborativas y aplicaciones de red open source y licenciadas, logrando un buen equilibrio entre la eficiencia de detección de situaciones o recuperación de información después de alguna incidencia o catástrofe de riesgo y privacidad de la información. A través de estos la información solo es accesible a personas autorizadas; Incrementando las capacidades de aprendizaje y eficiencia sobre los funcionarios de la empresa, mejorando así la ergonomía del sistema obteniendo beneficios para cada una de las áreas involucradas en la trazabilidad de los proyectos.

Gracias a la explotación de la tecnología y la transferencia de información generada a través de los proyectos aquí descritos, las empresas se verán fortalecidas al final de estos ya que la experiencia adquirida redundará en la formación de recursos tecnológicos y humanos. Por esta razón, se justifica la implementación de soluciones libres y de pago con arquitectura cliente-servidor de acuerdo a la necesidad de cada empresa para la productividad de los usuarios y continuidad del negocio.

4. MARCO TEÓRICO

Teniendo en cuenta la finalidad de estos proyectos basada en la implementación de herramientas de software libre y la cual suple las necesidades de las empresas "confidencialidad, integridad y disponibilidad" y frente a la seguridad teniendo en cuenta la reducción en la inversión de dinero es necesario contextualizar al lector acerca del papel que cumple cada elemento utilizado o factor estudiado antes de profundizar en cada una de las etapas.

4.1 Proyecto 1 Migración servidor Base de datos PostgreSQL

Concepto:
Una base de datos es una colección de información organizada de forma que un programa de ordenador pueda seleccionar rápidamente los fragmentos de datos que necesite. Una base de datos es un sistema de archivos electrónicos.[30]

Características:[31]

- Independencia de los Datos. Es decir, que los datos no dependen del programa y por tanto cualquier aplicación puede hacer uso de los datos.
- Reducción de la Redundancia. Llamamos redundancia a la existencia de duplicación de los datos, al reducir ésta al máximo conseguimos un mayor aprovechamiento del espacio y además evitamos que existan inconsistencias entre los datos. Las inconsistencias se dan cuando nos encontramos con datos contradictorios.
- Seguridad. Un SBD debe permitir que tengamos un control sobre la seguridad de los datos.
- Se visualiza normalmente como una tabla de una hoja de cálculo, en la que los registros son las filas y las columnas son los campos, o como un formulario.
- Permite realizar un listado de la base de datos.
- Permiten la programación a usuarios avanzados.

Tipos de base de datos:

Bases De Datos Estáticas:[32]

30 http://www.slideshare.net/jucajillo/base-de-datos-4954227

31 http://www.grupocto.es/tienda/pdf/en_opeval_capm.pdf

32 http://basededatos.over-blog.net/article-tipos-de-bases-de-datos-68319538.html

Estas son bases de datos de solo lectura, utilizadas primordialmente para almacenar datos históricos que posteriormente se pueden utilizar para estudiar el comportamiento de un conjunto de datos a través del tiempo, realizar proyecciones y tomar decisiones.

Bases De Datos Dinámicas:

Estas son bases de datos donde la información almacenada se modifica con el tiempo, permitiendo operaciones como actualización, borrado y adición de datos, además de las operaciones fundamentales de consulta. Un ejemplo de esto puede ser la base de datos utilizada en un sistema de información de un supermercado, una farmacia, un videoclub o una empresa.

Licenciamiento:[33]

Licenciado de tal manera que los usuarios pueden estudiar, modificar y mejorar su diseño mediante la disponibilidad de su código fuente. Bajo la Definición Open Source, las licencias deben cumplir diez condiciones para ser consideradas licencias de software abierto:

a) Libre redistribución: el software debe poder ser regalado o vendido libremente.
b) Código fuente: el código fuente debe estar incluido u obtenerse libremente.
c) Trabajos derivados: la redistribución de modificaciones debe estar permitida.
d) Integridad del código fuente del autor: las licencias pueden requerir que las modificaciones sean redistribuidas solo como parches
e) Sin discriminación de personas o grupos: nadie puede dejarse fuera.
f) Sin discriminación de áreas de iniciativa: los usuarios comerciales no pueden ser excluidos.
g) Distribución de la licencia: deben aplicarse los mismos derechos a todo el que reciba el programa.
h) La licencia no debe ser específica de un producto: el programa no puede licenciarse solo como parte de una distribución mayor.
i) La licencia no debe restringir otro software: la licencia no puede obligar a que algún otro software que sea distribuido con el software abierto deba también ser de código abierto.

33 http://es.wikipedia.org/wiki/C%C3%B3digo_abierto

j) La licencia debe ser tecnológicamente neutral: no debe requerirse la aceptación de la licencia por medio de un acceso por clic de ratón o de otra forma específica del medio de soporte del software.

4.2 Proyecto 2 Instalación y configuración consola Acronis Backup & Recovery

Concepto:
Acronis Backup & Recovery® 11.5 Universal Restore es un aplicativo totalmente integrado que restaura servidores o estaciones de trabajo a una configuración diferente de hardware o a una máquina virtual.

Características:[34]

- Programación avanzada de copia de seguridad: Especifique marcos de tiempo, frecuencia e intervalos para cada tipo de datos y cada tipo de máquina. Ajuste los parámetros para admitir diversas prioridades de copia de seguridad, sea para bases de datos que cambian rápidamente o almacenes de datos relativamente estáticos.
- Instantáneas de disco activas con soporte de bases de datos y aplicaciones de servidor.
- Acronis Backup & Recovery toma una 'instantánea' del disco utilizando las tecnologías patentadas de imágenes de disco de Acronis, lo que elimina la necesidad de desconectar un servidor para realizar una copia de seguridad.
- Restauraciones totalmente fiables con validación mejorada de archivos comprimidos.
- La validación mejorada de archivos comprimidos confirma que las copias de seguridad son completas y que se podrán recuperar tanto el servidor como los datos.
- Recupera un sistema entero o un solo archivo o carpeta: Las recuperaciones basadas en imágenes de Acronis le dan la granularidad de recuperación que necesita y le permiten volver a la actividad empresarial rápidamente. Los sistemas operativos, las aplicaciones y todos los datos pueden recuperarse por completo en cuestión de minutos, en lugar de horas o días.

34 http://www.ibotme.com/crea-copias-de-seguridad-de-sistema-con-acronis-backup-y-recovery-server/

- Una tecnología de cifrado avanzada garantiza la seguridad de los datos: Proporciona la protección de datos adicional que necesita con los algoritmos facilitados que son estándar en el sector o sus propias variantes personalizadas.
- Una tecnología de copia de seguridad de servidor optimizada y basada en imágenes maximiza el rendimiento de la copia de seguridad Basado en las tecnologías patentadas de imágenes de disco y restauración desde cero, Acronis Backup & Recovery captura una imagen de un disco y consolida los datos en un único archivo comprimido.

Licenciamiento:[35]

Las ediciones autónomas están diseñadas para realizar la copia de seguridad de datos en un único equipo. Con cualquiera de las licencias, puede instalar todos los componentes del producto en el mismo equipo. Se le pedirá la clave de licencia para cualquiera de las ediciones durante la instalación del producto.

Ediciones avanzadas (ediciones con gestión centralizada)

Estas son las siguientes ediciones:

Acronis Backup & Recovery 11.5 Advanced Server
Acronis Backup & Recovery 11.5 Virtual Edition
Acronis Backup & Recovery 11.5 Advanced Server SBS Edition
Acronis Backup & Recovery 11.5 Advanced Workstation

Estas ediciones están diseñadas para realizar la copia de seguridad de múltiples equipos. Además de los componentes que necesita instalar en un equipo incluido en la copia de seguridad, estas ediciones incluyen el servidor de gestión que permite la gestión centralizada y los nodos de almacenamiento para almacenar los datos incluidos en la copia de seguridad en los mismos. A diferencia de las ediciones autónomas, las ediciones avanzadas permiten la conexión remota a un equipo incluido en la copia de seguridad.
Al igual que con las ediciones autónomas, se necesita una licencia individual para cada equipo que desee incluir en la copia de seguridad. Durante la instalación del componente con licencia (agente), puede especificar un servidor de licencias o introducir una clave de licencia manualmente. No se requieren licencias para la

35 http://www.acronis.com/es-es/support/documentation/ABR11.5/index.html#13689.html

instalación de otros componentes. Por ejemplo, puede instalar tantos nodos de almacenamiento como desee, hasta 50.

4.3 Proyecto 3 Migración a Zimbra Collaboration Suite

Concepto:[36]
Zimbra es una solución completa de correo electrónico corporativo y colaboración con Antivirus y Antispam Es una suite de correo electrónico mensajería y colaboración innovadora. Soporta correos electrónicos y calendarios a través de una impresionante interfaz web Ajax, que provee tips de sus objetos, ítems arrastrables, y menús que se expanden al hacer clic derecho. También incluye capacidades de búsqueda avanzada y permite relacionar fechas
Características: El servidor ZCS hace uso de proyectos de código abierto existentes como Postfix, MySQL, OpenLDAP y Lucene. Cuenta con una interfaz de programación de aplicaciones basada en SOAP para toda su funcionalidad y actúa como servidor IMAP y POP3 de correo electrónico.
El cliente web ZCS es una interfaz de colaboración y administración completa creada empleando el Toolkit Zimbra. Soporta correos electrónicos y calendarios a través de una interfaz web basada en AJAX.
ZCS es compatible con clientes propietarios tales como Microsoft Outlook, Novell Evolution y Apple Mail. También provee soporte de sincronización nativo de dos vías para muchos dispositivos móviles: Nokia serie E, BlackBerry y Blackeberry Enterprise Server, Windows Mobile, entre otros.

Tipos de Licenciamiento:[37]

Open Source Edition: Totalmente funcional pero con algunos recortes en el interfaz Web y en la herramienta de administración. Este producto, se ofrece sin garantías y sin opción de adquirir soporte por parte del fabricante.

Network Profesional Edition (ZCS): La opción profesional, con funciones adicionales tanto en el interfaz Web, como en la herramienta de administración. Este tipo de versión, va acompañado por un soporte del fabricante y unas garantías del producto

Tipos de Licencia

36 http://es.scribd.com/doc/92907849/Zimbrapdf#scribd

37 http://observatorio.cds.gov.co/adjuntos/10.listadoComparacionCorreoElectronico.pdf

Anual: Este tipo de licencia permite usar Zimbra durante el periodo de un año. Antes de que finalice dicho periodo, es necesario renovar la licencia para que el sistema continúe funcionando. El coste de este tipo de licencia es aproximadamente de unos 25€ buzón por año. El mantenimiento y las actualizaciones por parte del fabricante Zimbra van incluidas en el precio de la adquisición de las licencias

Perpetua: Este tipo de licencia permite al cliente, adquirir la licencia de Zimbra en un único pago. El coste de dicha licencia viene a ser alrededor de 48€ por buzón. A este coste se le debe de agregar un 20% en concepto de soporte y actualizaciones de Zimbra.

4.4 Proyecto 4 Instalación - configuración de LogAnalyzer y Sophos UTM

Concepto:[38]
Gestión Unificada de Amenaza con una completa gama de aplicaciones de seguridad que incluye cortafuegos, VPN, IPS, seguridad de correo electrónico, filtrado web y control de aplicaciones

Sophos UTM Características:[39]

- Funciones de red:
- Firewall. Es un firewall de inspección de estado.
- Intrusión Prevention (IPS). Permite la prevención de intrusiones mediante el escaneo en tiempo real de los paquetes de red. Incorpora la actualización automática cada pocos minutos de las amenazas conocidas.
- DoS Protection. Es la protección para DoS (denegación de servicio), DDoS (denegación distribuida de servicio), escaneo de puertos, gusano y botnet.
- Directory Authentication. Además de la autenticación propia (local) de Sophos UTM, permite la autenticación basada en Active Directory de Microsoft. Pero no para todas las funciones, autenticación basada en Radius, LDAP y autenticación de Novell.
- UserPortal. Es el portal de usuarios finales, es decir, el usuario que accede a internet o a las redes protegidas por el firewall Sophos UTM. Permite a los usuarios obtener su configuración VPN, y algunas otras opciones.

38 http://www.xnetworks.es/contents/Sophos/sophos-utm-overview-dses.pdf

39 https://blogastaro.wordpress.com/2010/04/26/caracteristicas-principales-de-astaro/

- seguridad web (navegación web)
- URL Filtering. Control del acceso mediante urls, por categorías, por reputación, por franja horaria, por usuarios (con diferentes tipos de autenticación), para los protocolos http, https y ftp.
- IM/P2P Filtering. Controla los principales herramientas de chat (AIM, ICQ, MSN, Skype, Yahoo, IRC, Gtalk, Jabber) y P2P (peer-to-peer) (Bittorrent, Gnutella, eDonkey, WinMX, Winny, Manolita, Ares).
- Cache. Incluye cache web para mejorar la rapidez en el acceso web a internet.

- Correo electrónico:
- Escaneo de tráfico de entrada y salida (SMTP y POP3).
- Técnicas para la detención de correo electrónico no deseado (spam) como la Detección de Patrón Recurrente (Recurrent Pattern Detection), marcado en listado gris (grey-listing), RBL, patrón, heurística, SPF, BATV, URLs y listas B/W.
- Antivirus con dos motores.
- Email Encryption
- Codificación, decodificación y firma digital de correos electrónicos SMTP.
- Escaneo de correos electrónicos codificados, anexos comprimidos y codificados.
- Soporte para OpenPGP, S/MIME y estándares de codificación TLS.

- Administración y mantenimiento
- Administración vía web (https) y SSH. Esto permite una administración web rapidez en la consola.
- informes. Permite la monitorización del dispositivo en tiempo real y mediante se puede exportar informes en diferentes formato (HTML, PDF), Este tipo de informes puede ser enviado mediante correo electrónico periódicamente (semanal, mensual, etc.).
- Copias de seguridad (backup). Permite realizar copias de seguridad de forma fácil, tanto en la creación de las copias de seguridad como en la restauración posterior. Permite almacenar las copias de seguridad en el propio dispositivo, descargarlas con un navegador, o programarlas para que se envíen periódicamente por medio de correo electrónico.
- Funcionamiento en clúster. Permite el funcionamiento en clúster, tanto en modo activo-pasivo como en modo activo-activo.

Licenciamiento: Subscripción por módulos.

Servidor LogAnalyzer

Concepto:
Centralizar y consolidar archivos de log's de manera remota por diferentes dispositivos en la red que sean capaces de generar log's.

- Características
- Módulo reportes: Se consolidan los datos de eventos de rsyslog y otras proporcionando una facilidad de lectura.
- Escrito en PHP.

Licenciamiento: Licencia GPL.

4.5 Proyecto 5 Instalación y configuración servidor firewall pfSense

Concepto: [40]
PfSense es una aplicación que se instala como un sistema operativo ya que tiene varias funcionalidades entre estos servicios de redes LAN, WAN y servicios.

Características:

Firewall: Es un software o hardware que comprueba la información procedente de Internet o de una red y, a continuación, bloquea o permite el paso de ésta al equipo, en función de la configuración del firewall.

Network Address Translation (NAT): Network Address Translation o Traducción de Dirección de Red. Estándar para la utilización de una o más direcciones IP para conectar varias computadoras a una red (especialmente Internet).[41]

40 http://www.slideshare.net/nike_x99/pfSense-35097296

41 http://es.wikipedia.org/wiki/Traducci%C3%B3n_de_direcciones_de_red

VPN que puede ser configurada en IPsec, OpenVPN y en PPTP: Una VPN o Red Privada Virtual es una tecnología que permite la extensión de una red pública como Internet a un espacio de red local.[42]

Servidor DNS: Es una base de datos distribuida, con información que se usa para traducir los nombres de dominio, fáciles de recordar y usar por las personas, en números de protocolo de Internet (IP) que es la forma en la que las máquinas pueden encontrarse en Internet.[43]

Portal Cautivo: es una página Web con la cual un usuario de una red pública y/o privada debe interactuar antes de garantizar su acceso a las funciones normales de la red

Servidor DHCP: s un protocolo que permite que un equipo conectado a una red pueda obtener su configuración (principalmente, su configuración de red) en forma dinámica (es decir, sin intervención particular). Sólo tiene que especificarle al equipo, mediante DHCP, que encuentre una dirección IP de manera independiente. El objetivo principal es simplificar la administración de la red. PfSense cuenta con un gestor de paquetes para ampliar sus funcionalidades, al elegir el paquete deseado el sistema automáticamente lo descarga e instala.[44]

Licenciamiento:
pfSense is Copyright 2004-2015 Electric Sheep Fencing LLC Current logo is Copyright 2005-2015 Electric Sheep Fencing LLC, la redistribución y el uso en formas fuente y binario, con o sin modificaciones, están permitidos siempre que se cumplan las siguientes condiciones:

- Las redistribuciones del código fuente deben conservar la nota de copyright anterior, esta lista de condiciones y el siguiente descargo de responsabilidad.
- Las redistribuciones en formato binario deben reproducir el aviso de copyright anterior, esta lista de condiciones y el siguiente descargo de responsabilidad en la documentación y / u otros materiales proporcionados con la distribución.[45]
- Todo el material publicitario que mencione las funciones o el uso de este software debe mostrar el siguiente reconocimiento:

42 http://www.definicionabc.com/tecnologia/vpn.php

43 http://www.desarrolloweb.com/faq/50.php

44 http://es.kioskea.net/contents/261-el-protocolo-dhcp

45 https://www.pfSense.org/about-pfSense/

"Este producto incluye software desarrollado por el Proyecto de pfSense para su uso en la distribución de software pfSense®. (http://www.pfSense.org/). "
Los nombres "pfSense" y "Proyecto pfSense" no se deben utilizar para respaldar o promocionar productos derivados de este software sin permiso previo y por escrito. Para obtener permiso por escrito, póngase en contacto con legal@pfSense.org.

5. DESARROLLO DEL PROYECTO

5.1 Descripción de la situación actual

A continuación se describe la situación actual para cada uno de los proyectos realizados:

5.1.1 Proyecto 1 Migración servidor Base de datos PostgreSQL

En las instalaciones de la empresa PROSEGUROS S.A.CORREDORES DE SEGUROS se encuentra un servidor PostgreSQL sobre un servidor RHEL 6.3 el cual se encuentra en buenas condiciones pero el ingeniero de la empresa solicita crear un servidor imagen para realizar el traslado del servidor a la nueva sucursal el cual es para prevenir la pérdida o destrucción de la información.

5.1.2 Proyecto 2 Instalación y configuración consola Acronis Backup & Recovery

En la empresa Vansolix S.A se encuentra instalado un servidor de backup con una herramienta open source llamada Bacula pero no está cumpliendo a cabalidad las funciones que se requieren y con una administración muy compleja causando soportes y realizando llamadas a el proveedor constantemente para solucionar el incidente además a eso no se tiene confiabilidad sobre el producto.

5.1.3 Proyecto 3 Migración a Zimbra Collaboration Suite

En la empresa Víctor Manuel López (VML) se tiene instalado un servidor Fedora 15 con un servicio de postfix el cual tiene problemas de administración de la plataforma como lo es la administración de listas de distribución, spam, usuarios, espacio de buzón para los usuarios y restricciones del mismo.

5.1.4 Proyecto 4 Instalación - configuración de LogAnalyzer y Sophos UTM

En la empresa Sistemas Productivos SIPRO se tiene instalado un servidor pfSense el cual tiene como servicios (proxy, reglas de firewall, VPN (host to LAN)), también

se tiene una sociedad con una entidad financiera en la cual se realizó un auditoria interna y se estableció que como mejora se debe renovar el método de conexión por medio de VPN y el cifrado de correo electrónico que es transmitido a través del servidor firewall e implementar un servidor para almacenar los registro de log's de cada uno de los dispositivos en la red.

5.1.5 Proyecto 5 Instalación y configuración servidor firewall pfSense

En la empresa NIVER S.A se tiene un servidor firewall "Clear OS" administrado por un externo y por temas de disponibilidad no se puede dar acceso oportuno al personal que requiera una conexión inmediata ya sea internet, conexiones VPN o conexiones remotas.

5.2 Requerimientos de la información

A continuación se describe la metodología utilizada para poder ejecutar cada uno de los proyectos

5.2.1 Proyecto 1 Migración servidor Base de datos PostgreSQL

El proyecto está fundamentado en el core del negocio de la empresa SkillNet la cual basa su trabajo en Sistemas Operativos Linux y herramientas de software libre, no se utilizaron manuales de migración ya que lo único que se realizó fueron pruebas de migración antes de su implementación.

5.2.2 Proyecto 2 Instalación y configuración consola Acronis Backup & Recovery

El proyecto es ofrecido por solicitud del cliente en la cual se buscó el mejor producto por parte del departamento comercial de la empresa SkillNet, se ofreció confiabilidad, fácil administración y despliegue. En la solicitud se da una demo de 30 días para probar sus ventajas en el cual toda la configuración fue basada sobre manuales de administración y algunas colaboraciones del proveedor para tener los mejores resultados del producto hacia el cliente.

5.2.3 Proyecto 3 Migración a Zimbra Collaboration Suite

La información para realizar la migración de la plataforma de correo electrónico es extraída de la página de soporte y de la comunidad de Zimbra.

5.2.4 Proyecto 4 Instalación - configuración de LogAnalyzer y Sophos UTM

La instalación de la herramienta LogAnalyzer es extraída de la comunidad en el cual solo se brinda el proceso de instalación. El manejo de la herramienta es intuitivo de igual manera se brinda capacitación al personal que la va administrar, en cuanto a la plataforma de SOPHOS UTM es documentación publicada en internet por los fabricantes donde brindan la configuración de cada uno de los módulos.

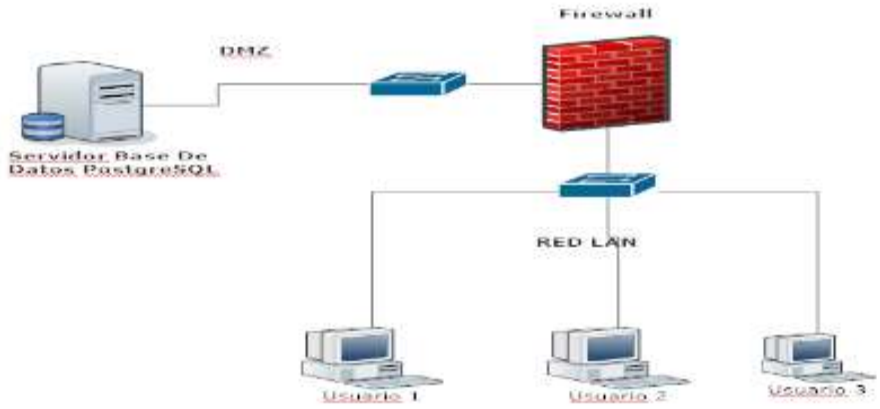
5.2.5 Proyecto 5 Instalación y configuración servidor firewall pfSense

La instalación y configuración fue realizada de video tutoriales y búsqueda de información sobre configuración. En el mercado no existe un manual donde explique la funcionalidad de cada módulo ya que esto es software libre.

5.3 Modelamiento del sistema

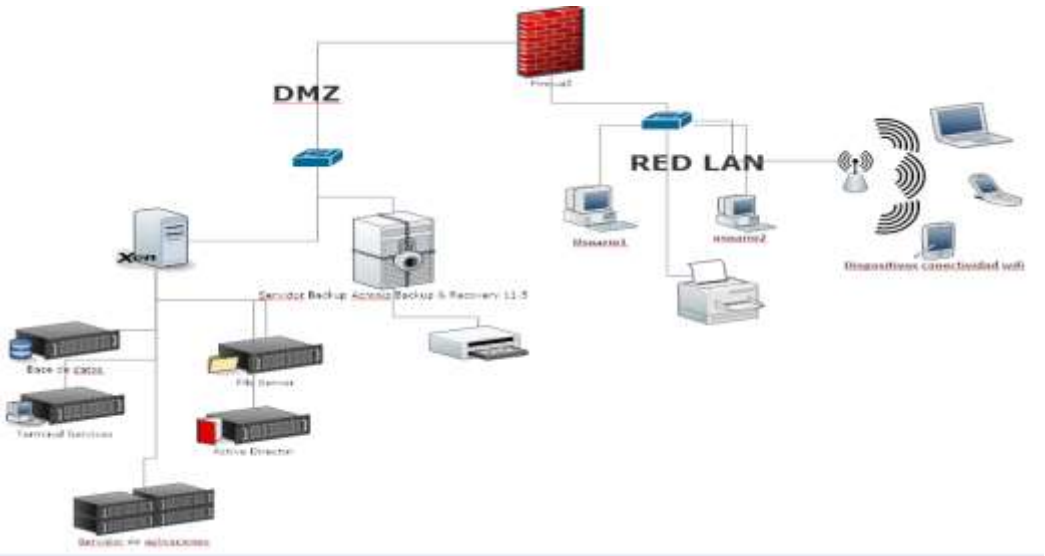
5.3.1 Proyecto 1 Migración servidor Base de datos PostgreSQL

Ilustración 1Diagrama de red base de datos PostgreSQL



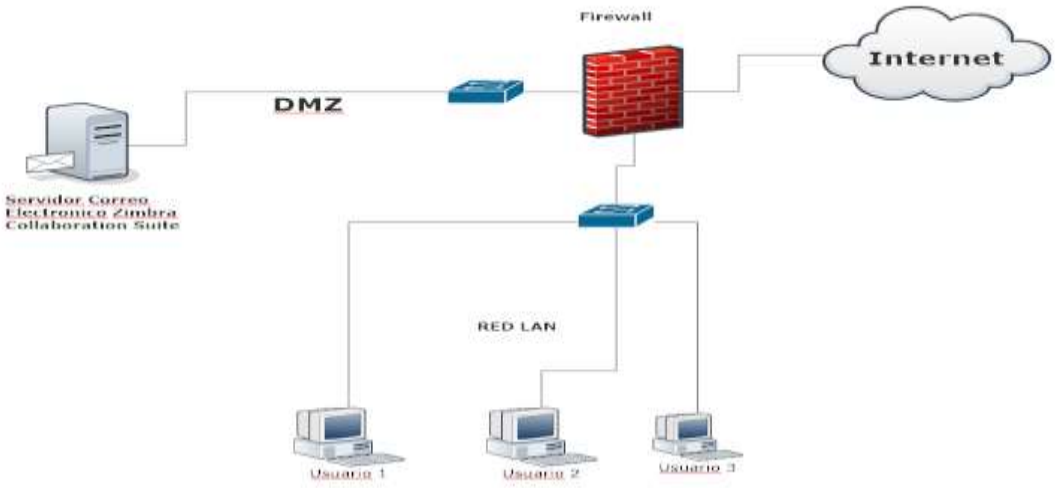
5.3.2 Proyecto 2 Instalación y configuración consola Acronis Backup & Recovery

Ilustración 2 Diagrama de Red implementación Acronis Backup & Recovery



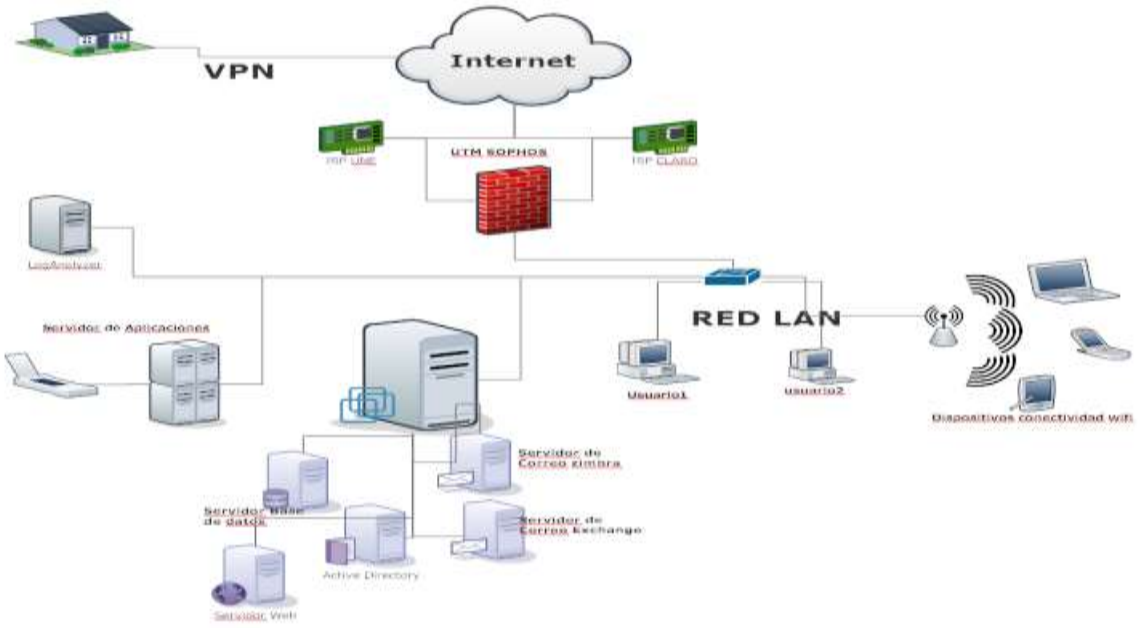
5.3.3 Proyecto 3 Migración a Zimbra Collaboration Suite

Ilustración 3 Diagrama de Red configuración Zimbra Collaboration Suite



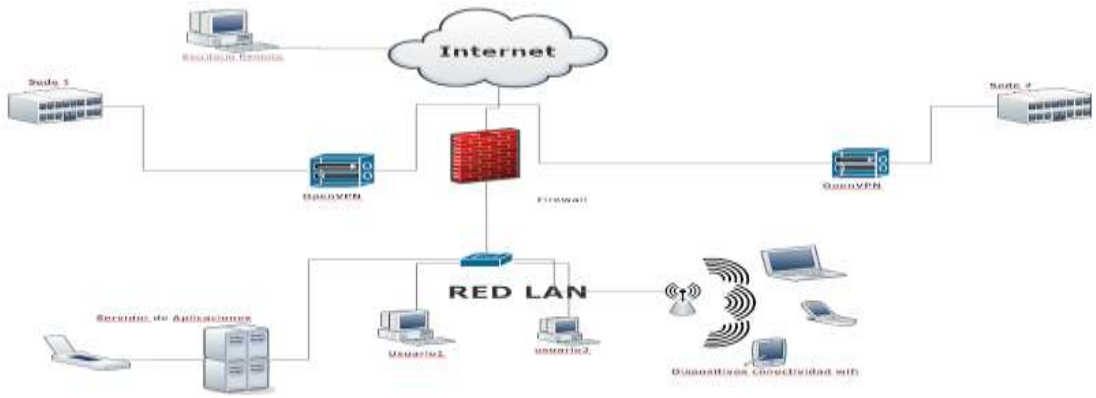
5.3.4 Proyecto 4 Instalación - configuración de LogAnalyzer y Sophos UTM

Ilustración 4 Diagrama de red Instalación-configuración de LogAnalyzer y Sophos UTM



5.3.5 Proyecto 5 Instalación y configuración servidor firewall pfSense

Ilustración 5 Diagrama de red Instalación y configuración servidor firewall pfSense



5.4 Descripción del sistema:

A continuación se da a conocer la descripción de cada uno de los proyectos implementados y el funcionamiento en la red.

5.4.1 Proyecto1 Migración servidor Base de datos PostgreSQL

Servidor Base De Datos PostgreSQL está configurado sobre sistema operativo RedHat con versión 6.3. El servidor se encuentra en una zona desmilitarizada en el cual el firewall es quien actúa como filtro para que solo pueda ser accedido desde la red LAN por el puerto 5432 (postgreSQL) en el cual el proceso es transparente para los usuarios por que se maneja un aplicativo el cual es el que realiza la conexión. Se tiene habilitado el puerto 22 (SSH) solo desde la IP del ingeniero responsable del servidor.

5.4.2 Proyecto 2 Instalación y configuración consola Acronis Backup & Recovery

Se tiene una zona desmilitarizada (DMZ) en el cual está disponible una virtualización sobre Citrix Xencenter y se tienen alojados servidores de FTP, Directorio Activo, File Server, Terminal Services, Bases de Datos, Servidor de Aplicaciones entre otros. Todos los usuarios de la red LAN trabajan con recursos compartidos sobre algunos servidores. El servidor Backup Acronis Backup & Recovery 11.5 actúa como servidor para realizar copias de seguridad y sobre cada uno de los servidores se instala un agente y se configuran políticas según nivel de criticidad del servicio para ser resguardadas ya sea en cintas o discos duros.

5.4.3 Proyecto 3 Migración a Zimbra Collaboration Suite

El servidor de correo Zimbra Collaboration Suite está configurado sobre un sistema operativo CentOS con versión 6.5, dicho servidor se encuentra en una zona desmilitarizada(DMZ) en el cual el firewall es quien actúa como filtro para que sea accedido desde la red LAN e internet a través de los puertos 25 (SMTP), 110(IMAP), 143(POP), 993(POP3S), 995(IMAPS), 445(SMTPS), 587(SMTPS), 80(http) y 443 (https).

5.4.4 Proyecto 4 Instalación - Configuración de LogAnalyzer y Sophos UTM.

En diagrama de red se observa que se tienen servidores virtualizados con VMWare y un firewall appliance Sophos UTM donde cada uno de ellos están realizando envió de registros al servidor de log's (LogAnalyzer) el cual está diseñado para aceptar controlar y mantener evidencia de los procesos realizados en los servidores o aplicaciones de la organización.

La empresa tiene contratado dos proveedores de internet en el cual el firewall appliance Sophos UTM es el encargado de gestionar las direcciones IP públicas las cuales están configuradas para hacer balanceo de cargas para mitigar riesgos de conectividad a internet y tener siempre disponibilidad del servicio. El servidor firewall Sophos UTM actúa como puerta de enlace tanto de la red LAN e inalámbrica para hacer el filtro de navegación a internet de los usuarios donde se tienen módulos embebidos con motores de antivirus para prevenir la descarga de archivos maliciosos o páginas vulneradas con PHISHING, también se tiene control de correos con virus y están siendo escaneados en el servidor para poder hacer relay a su respectivo servidor de correo. Se tienen módulos de acceso remoto por medio de VPN ya sea por software o HTML5.

5.4.5 Proyecto 5 Instalación y configuración servidor firewall pfSense

Se tiene un servidor de aplicaciones donde cada una de las sedes deben tener acceso a él por medio de un cliente para gestionar los procesos, el servidor firewall PfSense actúa como puerta de enlace para la conectividad por medio de VPN (site to site) sobre cada una de las sedes, de igual forma no solo controla el ingreso al aplicativo si no también el control de acceso a internet de una manera centralizada ya sea para las redes inalámbricas o cableadas.

6 EVALUACIÓN ECONÓMICA DEL PROYECTO

6.1 Riesgo en fase de análisis

Lo riesgos encontrados durante la fase de análisis en los proyectos se identificaron de la siguiente manera:

6.1.1 Proyecto1 Migración servidor Base de datos PostgreSQL

- Pérdida de información.
- Conexión por permisos a la base de datos.
- Permisos de conectividad a la base de datos por políticas de denegación en el firewall.

6.1.2 Proyecto 2 Instalación y configuración consola Acronis Backup & Recovery

- No contar con los permisos suficientes para poder realizar las copias de seguridad sobre los archivos.
- Al momento de restaurar una copia de seguridad no se encuentre la información solicitada.
- Los drivers de la unidad de tape no sean compatibles con el Sistema Operativo.

6.1.3 Proyecto 3 Migración a Zimbra Collaboration Suite

- Pérdida de información en el momento de la sincronización de los correos por medio de imapsync.
- El hardware este defectuoso.

6.1.4 Proyecto 4(Instalación - configuración de LogAnalyzer y Sophos UTM

- Denegar el acceso a internet a los usuarios.

- Los dispositivos no tengan módulo de log's para él envió remoto.
- Falla o daño en los equipos de cómputo o comunicación.

6.1.5 Proyecto 5 Instalación y configuración servidor firewall pfSense

- El hardware no sea compatible con la versión del Sistema Operativo.
- Denegar el acceso a internet a los usuarios.

6.2 Riesgo en fase de diseño

Lo riesgos encontrados durante la fase de diseño en los proyectos referentes a tiempos, presupuestos, disponibilidad actores o recursos necesarios se identificaron de la siguiente manera.

6.2.1 Proyecto 1 Migración servidor Base de datos PostgreSQL

- Desactualización en avances tecnológicos, tanto en hardware como en software.
- Retraso en cronograma de actividades.

6.2.2 Proyecto 2 Instalación y configuración consola Acronis Backup & Recovery

- Diseño inadecuado (hay que volver a diseñar).
- Inadecuado almacenamiento de la información, por cuanto no existe el sitio adecuado.
- Falla o daño en los equipos de cómputo o comunicación.
- Accesos no autorizados a los recursos tecnológicos.
- Retraso en el cronograma de actividades

6.2.3 Proyecto 3 Migración a Zimbra Collaboration Suite

- Entrada de programas malignos como virus, malware, troyanos, spyware o spam, acceso no autorizados.
- No se cuenta con el área de tecnología o informática en la organización.
- No se cuenta internet para la descarga de paquetes necesarios.

6.2.4 Proyecto 4 Instalación - configuración de LogAnalyzer y Sophos UTM

- Entrada de programas malignos como virus, malware, troyanos, spyware, correo spam.
- No se cuenta con disponibilidad del ingeniero de la empresa.

6.2.5 Proyecto 5 Instalación y configuración servidor firewall pfSense

- Los recursos no están disponibles en su momento.
- Seguridad deficiente.
- No se tenía muchos conocimientos de la infraestructura de la empresa

6.3 Riesgo en fase de pruebas

Lo riesgos encontrados durante la fase de pruebas en los proyectos se identificaron de la siguiente manera:

6.3.1 Proyecto 1 Migración servidor Base de datos PostgreSQL

- La versión del sistema operativo estaba en beta lo cual la base de datos no estaba disponible con la misma versión.
- No se tenía el control de acceso adecuado para la base de datos estaba accesible para toda la red LAN.

6.3.2 Proyecto 2 Instalación y configuración consola Acronis Backup & Recovery

- La unidad de cinta LTO pierde conectividad.
- El sistema operativo no tiene licencia para realizar actualización de parches.
- Se genera error cada vez que se realiza una copia de seguridad por falta de permisos sobre el agente configurado en el servidor cliente.

6.3.3 Proyecto 3 Migración a Zimbra Collaboration Suite

- La sincronización con el comando “rsync” no funciona por falta de dependencias.

- Los contactos no se exportan después de la migración.
- La IP pública que se estaba utilizando estaba reportada en listas negras de internet el cual se tuvo que solicitar el cambio de IP y registros DNS.

6.3.4 Proyecto 4 Instalación - configuración de LogAnalyzer y Sophos UTM

Sophos UTM:

- Problemas de autenticación en el directorio activo.
- El servidor de correo Exchange interno no envía ni recibe correos a través de la SOPHOS UTM.

LogAnalyzer:

- La máquina tiene poco recursos para administrar los log's de 8 servidores.
- Máquina obsoleta.

6.3.5 Proyecto 5 Instalación y configuración servidor firewall pfSense

- El firewall pfSense instalado no es compatible con la tarjeta de red sobre la máquina entregada por el cliente.
- Instalación de versión beta pfSense.
- No se tiene seguridad física.
- Problemas de ingreso con páginas SSL.

6.4 Riesgo en fase de implementación

Lo riesgos encontrados durante la fase de implementación en los proyectos se identificaron de la siguiente manera

6.4.1 Proyecto 1 Migración servidor Base de datos PostgreSQL

Permisos de acceso desde la red LAN al servidor instalado y configurado, no se cuenta con permisos en la red para gestionar las bases de datos el cual está siendo controlada por el administrador de Firewall.

6.4.2 Proyecto 2 Instalación y configuración consola Acronis Backup & Recovery

- Desconexión unidad de tape.
- Incompatibilidad en el sistema operativo y dispositivo externo unidad de cinta LTO.

6.4.3 Proyecto 3 Migración a Zimbra Collaboration Suite

- No se tenía preparada la dirección IP pública al momento de la puesta en marcha.
- Configuración de certificados SSL sobre clientes Outlook.

6.4.4 Proyecto 4 Instalación - configuración de LogAnalyzer y Sophos UTM

- Control de acceso de usuarios a internet.
- Tabla ARP de la capa de enlace tiene una identificación diferente para el nuevo dispositivo de red el cual va a ocupar una IP ya existente.

6.4.5 Proyecto 5 Instalación y configuración servidor firewall pfSense

- Control de acceso de usuarios a internet.
- No se han aplicado los cambios para los registros tipo AAA, MX y PTR por parte del ISP sobre la direcciones IP.

6.4 Riesgo en fase de mantenimiento

Lo riesgos encontrados durante la fase de mantenimiento en los proyectos se identificaron de la siguiente manera:

- Realizar un escaneo de vulnerabilidades interno y/o eterno antes de realizar la visita de mantenimiento.
- Realizar copia de seguridad antes de realizar cualquier cambio sobre la plataforma.

- Validar actualización de parches sobre los paquetes instalados.
- Cuando se realice una actualización no afectar las aplicaciones leer documentación.
- Tener suscripciones activas cuando el producto es con licencia de pago para poder mantener las actualizaciones del OS.
- Validar con el ingeniero responsable que problemas se tienen sobre la plataforma y corregirlos.
- Búsqueda de mejoras sobre la plataforma.
- Realizar informe de visita de mantenimiento y brindar recomendaciones de la plataforma.

7 Beneficios de la implementación

La organización en general se vuelve más competitiva al reaccionar efectiva y eficazmente conforme a las necesidades del negocio.

7.1 De Infraestructura

- Administración centralizada.
- Liberación de personal de IT en áreas de backup.
- Disminución de tiempos de inactividad.
- Reducción y control de riesgos.
- Optimizar recursos.
- Reducir costos.

7.2 De IT

- Suprimir la duplicidad de las actividades.
- Mejoras en la disponibilidad y seguridad brindadas por el área de IT.
- Estar a la vanguardia de la tecnóloga.
- Mejorar la calidad del servicio entregado al usuario de acuerdo a sus necesidades específicas.
- Mejora en la satisfacción del cliente y del usuario final.
- Fácil administración.

8. ALCANCE DEL PROYECTO

8.1 Proyecto 1 Migración servidor Base de datos PostgreSQL

- Instalación y configuración de un servidor con sistema operativo Linux con distribución Red Hat 6.3 para la instalación de postgreSQL.
- Clonar sistema operativo con base de datos.
- Pruebas de base de datos desde el aplicativo (insertar, eliminar, consultar y editar).
- Traslado de servidor a la sede donde estará en pruebas.
- Acompañamiento traslado y puesta en producción.
- No incluye ningún tipo de administración de la base de datos o servidor
- Garantía 3 meses.

8.2 Proyecto 2 Instalación y configuración consola Acronis Backup & Recovery

- Instalación sistema operativo Windows 2008 R2.
- Instalación consola Acronis Backup & Recovery 11.5.
- Configuración de 8 servidores con agente Acronis Backup & Recovery 11.5 para realizar copias de seguridad.
- Parametrización Acronis Backup & Recovery 11.5.
- Adicionar servidor Acronis Backup & Recovery 11.5 al directorio activo de la compañía.
- Acompañamiento para la creación de tareas (copias de seguridad)
- Capacitación de la herramienta
- Documentación
- No incluye ningún tipo de administración.
- 3 vistas de mantenimiento anuales.

8.3 Proyecto 3 Migración a Zimbra Collaboration Suite

- Instalación sistema operativo Linux CentOS 6.4.
- Instalación DNS enjaulado.
- Instalación de Zimbra Collaboration Suite versión 8.

- Migración de 150 cuentas de correo electrónico.
- Creación de listas y de Alias de correo electrónico.
- Afinamiento local de antivirus y anti spam.
- Instalación zimlet para el chat corporativo.
- Hardening servidor.
- Capacitación.
- No incluye ningún tipo de administración.

8.4 Proyecto 4 Instalación - configuración de LogAnalyzer y Sophos UTM

Alcance Sophos UTM

- Configuración Sophos UTM.
- Migración y depuración de políticas.
- Puesto en marcha.
- Afinamiento de la herramienta.
- Documentación de la herramienta implementada en la compañía.
- Capacitación a máximo 3 personas del área.
- 3 visitas de mantenimientos anuales, documentación.
- No se incluye ningún tipo de administración.

Alcance LogAnalyzer

- Instalación sistema operativo CentOS 6.5.
- instalación y configuración LogAnalyzer.
- Configuración RSYSLOG para 15 dispositivos (servidores y dispositivos de red).
- Hardening servidor.
- Documentación de la herramienta implementada en la compañía.
- Capacitación a máximo 3 personas del área.
- 3 visitas de mantenimientos anuales.
- No se incluye ningún tipo de administración.

8.5 Proyecto 5 Instalación y configuración servidor firewall pfSense

- Instalación firewall pfSense 2.0 RC1
- Configuración firewall con servicios (OPENVPN, DHCP, PROXY, Lightsquid, reglas LAN-NAT y WAN).
- Capacitación a máximo 3 personas del área.

- Documentación.
- Puesta en marcha.
- Afinamiento.
- 3 visitas de mantenimientos anuales.
- No se incluye ningún tipo de administración.

9. LIMITACIONES DEL PROYECTO

9.1 Proyecto 1 Migración servidor Base de datos PostgreSQL

- No se tiene licenciamiento RedHat para realizar actualizaciones de paquetes.

9.2 Proyecto 2 Instalación y configuración consola Acronis Backup & Recovery

- Se debe tener un agente instalado en cada uno de los servidores para realizar copias de seguridad.
- No se cuentan buenos recursos de hardware para su mejor rendimiento.
- No se puede restaurar las bases de datos en caso de pérdida cuando las copias de seguridad son a cinta.

9.3 Proyecto 3 Migración a Zimbra Collaboration Suite

- No se puede configurar las agendas en los clientes Outlook.
- No se pueden realizar o restaurar copias de seguridad desde la consola de administración.

9.4 Proyecto 4 Instalación - configuración de LogAnalyzer y Sophos UTM

- Los dispositivos inalámbricos no cuentan con el paquete de envió remoto de log'.
- No se permite la instalación de herramientas en la Sophos UTM.
- El servidor Sophos UTM no permite la administración de Access Point que no sean del mismo fabricante.
- No se tiene un buen rendimiento del servidor por falta de recursos.

9.5 Proyecto 5 Instalación y configuración servidor firewall pfSense

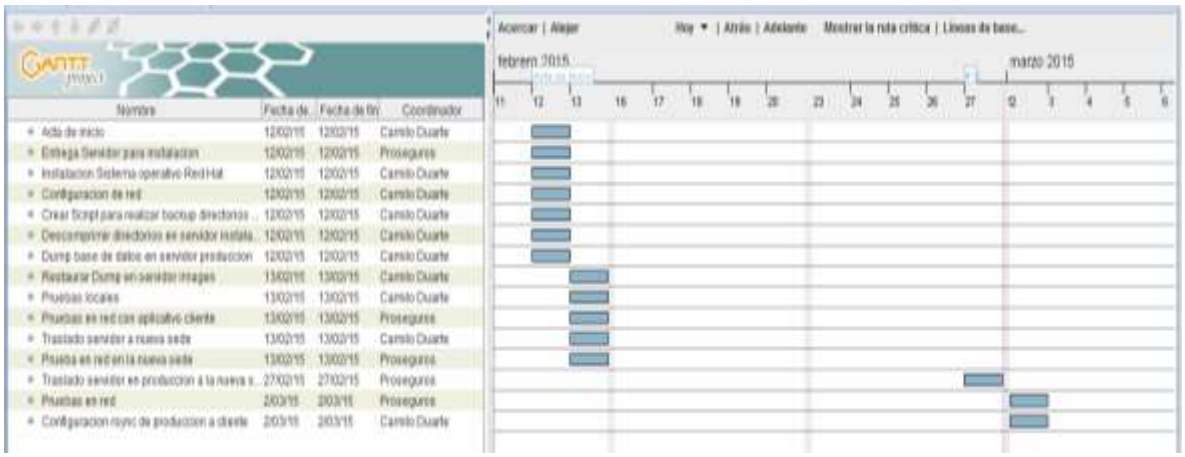
- No se permite la instalación de herramientas en el Sistema Operativo. Excepto las que se encuentran disponibles en los repositorios.
- No se tiene firewall en la capa de aplicación.

10. CRONOGRAMA

Por medio de una gráfica o tabla se puede mostrar el tiempo que tomó el desarrollo cada etapa de este trabajo.

10.1 Proyecto 1 Migración servidor Base de datos PostgreSQL

Tabla 1 Cronograma Migración servidor base de datos PostgresSQL



10.2 Proyecto 2 Instalación y configuración consola Acronis Backup & Recovery

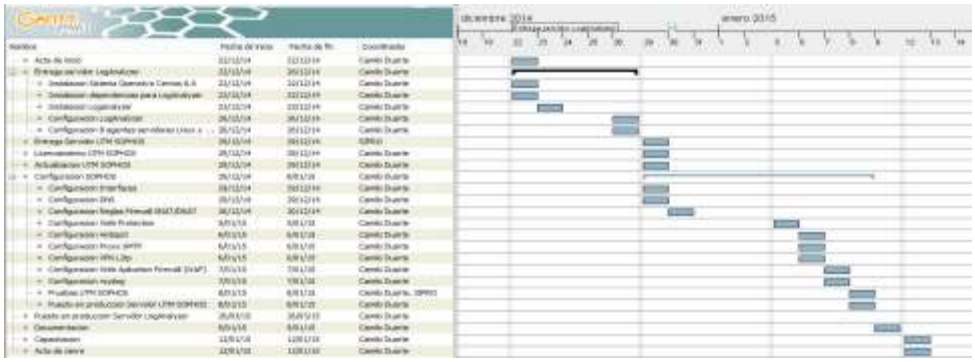
Tabla 2 Cronograma Instalación Configuración Consola Acronis Backup & Recovery

10.3 Proyecto 3 Migración a Zimbra Collaboration Suite

Tabla 3 Cronograma Migración a Zimbra Collaboration Suite

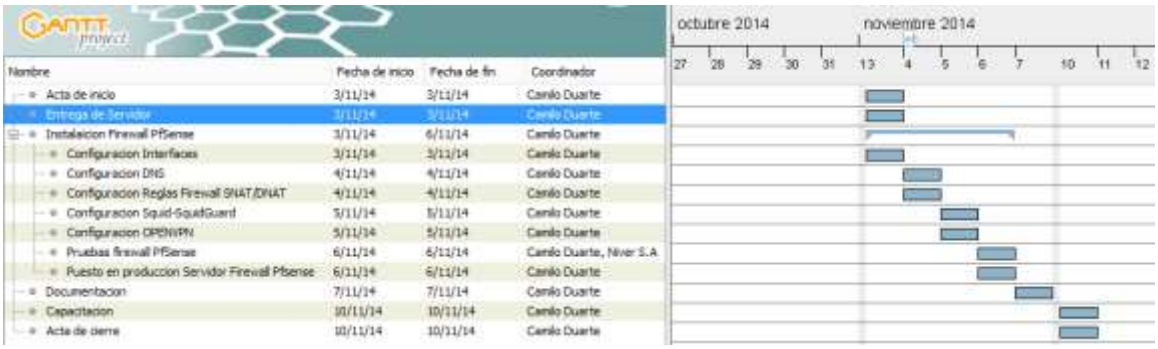
10.4 Proyecto 4 Instalación - configuración de LogAnalyzer y Sophos UTM

Tabla 4 Cronograma Instalación - configuración de LogAnalyzer y Sophos UTM



10.5 Proyecto 5 Instalación y configuración servidor firewall PfSense

Tabla 5 Cronograma Instalación y configuración servidor firewall PfSense



11. PRESUPUESTO

Tabla 6 Presupuesto para la ejecución de Proyectos

Item	Proyecto	Horas	Servidores	Cantidad	Licencia Pago	Licencia Libre	Valor Implementacion
1	Migración servidor Base de datos PostgreSQL	20	1	1		x	$ 9.700.000,00
2	Instalación y configuración consola Acronis Backup & Recovery	24	1	8 agentes	x		$ 13.400.000,00
3	Migración a Zimbra Collaboration Suite	24	1	150 cuentas		X	$ 4.900.000,00
4	Instalación - configuración Sophos UTM	62	1	FULL GUARD	x		$ 22.180.000,00
5	Instalación - configuración de LogAnalyzer	24	1	15 agentes		x	$ 3.800.000,00
6	Instalación y configuración servidor firewall PfSense	45	1	1		x	$ 4.800.000,00
Total Horas Trabajadas		199	6				**$ 58.780.000,00**

CONCLUSIONES

- Se implementó cada uno de los proyectos según la propuesta acordada.
- Se logró crear una administración mucho más fácil e intuitiva.
- Se planteó una metodología para la implementación de cada proyecto.
- Se consiguió mejorar la productividad de los usuarios mediante políticas de navegación.
- Se adquirió ganar fiabilidad sobre herramientas de código libre a bajo costo.
- Se logra optimizar y suprimir las actividades del área de tecnología.
- Se hallaron nuevos inconvenientes que pueden ser desarrollados en labores futuras.

RECOMENDACIONES

Proyecto 1 Migración servidor Base de datos PostgreSQL

- Se recomienda realizar un hardening al servidor en producción ya que al momento de realizar la migración se evidenciaron bastantes vulnerabilidades por ejemplo creación de políticas de uso de contraseñas, modificación de parámetros de red para denegar la aceptación de paquetes prevenir ataques DoS, implementación de firewall local.
- Obtener una suscripción de REDHAT para mantener actualizados los paquetes.

Proyecto 2 Instalación y configuración consola Acronis Backup & Recovery

- Realizar pruebas de recuperación periódicamente para validar la integridad de los datos.
- Mantener actualizado los parches tanto del sistema operativo como del aplicativo.

Proyecto 3 Migración a Zimbra Collaboration Suite

- Mantener actualizado los parches del sistema operativo y realizar un hardening de la plataforma de correo Zimbra Collaboration Suite.
- Realizar copias de seguridad de las cuentas de correo electrónico y sus archivos de configuración.
- Implementar un servidor de respaldo para realizar una sincronización de archivos de configuración y buzones de usuarios.

Proyecto 4 Instalación - configuración de LogAnalyzer y Sophos UTM

- Mantener aislado el servidor logAnalyzer y tener buen control de contraseñas para el ingreso de este servidor.
- Aumentar la memoria para el servidor de log's ya que por el procesamiento de log's se torna lento la evagación en la plataforma.
- Realizar un análisis de vulnerabilidades mínimo 3 veces al año para corregir agujeros de seguridad.

- Mantener actualizado los servidores.

Proyecto 5 Instalación y configuración servidor firewall pfSense

- Mantener actualizado el servidor firewall.
- Tener un servidor de respaldo para prevenir estar fuera de línea por mucho tiempo y afectar el funcionamiento de la organización.
- Realizar un análisis de vulnerabilidades mínimo 3 veces al año para corregir agujeros de seguridad.

WEBGRAFIA

Estanislao, L. (17 de 04 de 2007). *taringa.net*. Recuperado el 10 de 04 de 2015, de http://www.taringa.net/posts/offtopic/1114168/Licencia-Open-Source.html

basededatos.over-blog.net. (01 de 03 de 2011). Recuperado el 05 de 04 de 2015, de http://basededatos.over-blog.net/article-tipos-de-bases-de-datos-68319538.html

blogastaro. (26 de 04 de 2010). *blogastaro.wordpress.com*. Recuperado el 17 de 04 de 2015, de https://blogastaro.wordpress.com/2010/04/26/caracteristicas-principales-de-astaro/

es.wikipedia.org. (s.f.). Recuperado el 12 de 04 de 2015, de http://es.wikipedia.org/wiki/Zimbra

grupomitk. (05 de 03 de 2009). *es.slideshare.net*. Recuperado el 12 de 04 de 2015, de http://es.slideshare.net/grupomitk/proyecto-final-1380701

pfsense.org. (s.f.). Recuperado el 21 de 04 de 2015, de https://www.pfsense.org/about-pfsense/#legal

rafaelma. (02 de 10 de 2010). *postgresql.org.es*. Recuperado el 29 de 03 de 2015, de http://www.postgresql.org.es/sobre_postgresql

S.L, Q. s. (s.f.). *quersystem.com*. Recuperado el 12 de 04 de 2015, de http://www.quersystem.com/docs/Comparativa%20soluciones%20Groupware%20%28Zimbra,%20Open-Xchange,%20Scalix%29.pdf

seguridadinformaticaufps.wikispaces.com. (s.f.). Recuperado el 21 de 04 de 2015, de https://seguridadinformaticaufps.wikispaces.com/file/view/PFSENSE.pdf

smartdraw.com. (s.f.). Recuperado el 25 de 04 de 2015, de http://www.smartdraw.com/

sophos.com. (s.f.). Recuperado el 17 de 04 de 2015, de https://www.sophos.com/es-es/medialibrary/pdfs/factsheets/sophosutm220dsna.pdf

usbmed.edu.co. (s.f.). Recuperado el 21 de 04 de 2015, de http://www.usbmed.edu.co/index.php/component/content/article/9-uncategorised/137-edcontinua-seguridad-informatica-operativa%20%20%20-%3E%20Obj.%20especificos

Yumbla, C. (20 de 08 de 2009). *slideshare.net*. Recuperado el 3 de 04 de 2015, de http://www.slideshare.net/ceciliayumbla/investigacion-de-firewall

BIBLIOGRAFIA

- Korry Douglas, Susan Douglas. PostgreSQL, 2nd Edition. Julio 2005.
- Daniel L. Morrill. Configuración de sistemas Linux. Editorial Anaya Multimedia, 2002.
- Ariganello Ariganello, Ernesto. REDES CISCO: Guía de Estudio para la Certificación CCNA 640-802. 2ª edición. RA-MA EDITORIAL, 2011.
- Dee-Ann Leblanc. La Biblia de Administración de sistemas Linux. La Biblia de, Editorial Anaya Multimedia, 2001.
- Robert Ziegler y José Ignacio Sánchez. Guía Avanzada Firewalls Linux. 1ª edición, Editorial Prentice Hall PTR, 2001.
- Ruth Maran. Aprenda Red Hat Linux Visualmente (Serie Tridimensional). ST Editorial, 2001.