3. VALORACIÓN ECONÓMICA

3. VALORACIÓN ECONÓMICA

3.1 Modelo de negocio en el software libre

En esta sección, veremos cómo podríamos dar una salida comercial a todo el trabajo desarrollado en el presente proyecto y cómo invertir el "know-how" adquirido en la realización de proyectos reales y vendibles. Puede resultar paradójico a primera vista cómo es posible vender soluciones basadas en software libre si no tenemos que pagar ninguna licencia a ningún desarrollador o empresa por utilizarlo, realmente lo que ocurre es que se entiende el software como un servicio y no como un producto.

Las motivaciones de los desarrolladores así como los integradores de tecnologías basadas en software libre son muy variadas, aunque muchas aluden a ciertos principios anarquistas o a la posibilidad de formas mutualistas o de cooperación dentro del sistema capitalista, hay también quizás quienes consideran al software libre como la única oportunidad de competir en un mercado dominado por las grandes compañías de software propietario. ¿Pero dónde está el negocio para estas personas? ¿Cómo compiten y ganan dinero con el "open source"?

La ganancia más importante del open source está en la comercialización o en la entrega de servicios asociados. El cliente no debe pagar por usar el software sino por los servicios de asistencia técnica, de capacitación y por la implementación de nuevas características y la corrección de errores o defectos. Para muchos clientes esto significa un gran ahorro y una mayor independencia: no deben pagar licencias ni acceder a la piratería, y pueden adaptar completamente sus sistemas a sus necesidades. Y para el desarrollador del software, o el programador, o integrador de una empresa, la ventaja competitiva está en que tiene un considerable avance sobre los otros programadores a la hora de vender sus servicios o copar un nicho del mercado: estuvo involucrado en la creación o adaptación del software y por eso lo conoce mejor y puede trabajar de forma más rápida y eficiente.

Así pues, desarrollaremos el modelo de negocio de nuestro dispositivo Debian basándonos en la venta de servicios de configuración de las herramientas de red que hemos analizado, adaptándolas a las necesidades de nuestros clientes y ofreciendo un mantenimiento para garantizarles la disponibilidad de sus sistemas.

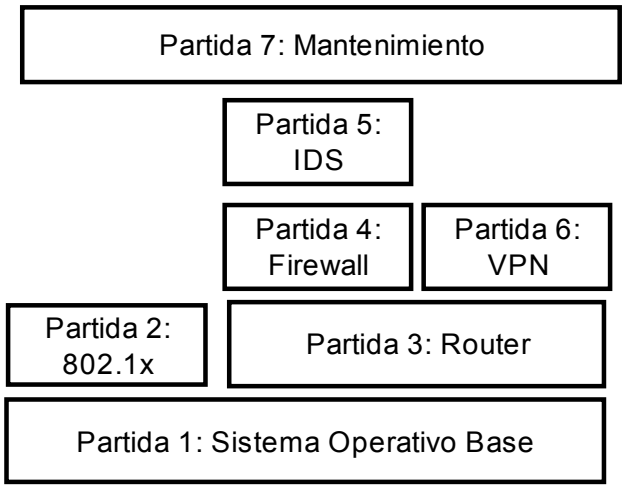
3.2 Presupuesto

En esta valoración económica, hemos fijado nuestro nicho de mercado a pequeños clientes, como pequeñas oficinas, PYMES o estudios de particulares con redes de área local que deseen proteger. No obstante, todas estas tecnologías son aplicables a escenarios de mayor envergadura, son altamente escalables y podrían dimensionarse según las necesidades del cliente.

Nos alejaríamos de esta manera de la visión que hemos tenido durante todo el proyecto sobre el estudio de nuestra máquina como un dispositivo aislado; ampliando así nuestro horizonte de posibilidades pudiéndolo utilizar dentro de complejos sistemas de telecomunicaciones como pudieran ser sistemas de alta disponibilidad, estructura de dispositivos en clústeres, cobertura inalámbrica extensa, integración con sistemas de monitorización, bases de datos y otras configuraciones avanzadas. Echando a volar nuestra imaginación por unos instantes, si fuéramos una empresa consultora e integradora de tecnologías de la información y comunicación, podríamos realizar infraestructuras de telecomunicaciones completas, donde la inteligencia de los dispositivos de red residiera en herramientas basadas en software libre.

Volviendo a nuestro planteamiento inicial, presentamos a continuación un modelo de presupuesto genérico dividido en distintas secciones o bloques, de tal manera que podríamos darle al cliente final una oferta completamente personalizada en función de si desea que su dispositivo desempeñe todas las funciones de red descritas o sólo aquellas que necesite.

En el diagrama de bloques representado adjunto observamos cómo hemos desglosado en diferentes partidas los distintos servicios que ofrecemos, de tal manera que el dispositivo se construye de abajo hacia arriba. Por ejemplo: si un cliente necesitara un Firewall con un servicio de mantenimiento, nuestro trabajo sería el proveerle de una máquina con un sistema base Debian instalado, la configuración de red y el encaminamento y posteriormente el cortafuegos según los requisitos de sus comunicaciones. Por tanto, le facturaríamos las partidas 1, 3, 4 y la parte correspondiente de la 7.



El desglose de las partidas es como sigue:

Partida 1. Hardware e Instalación del sistema operativo Debian			
Ud.	Concepto	Precio Unitario	SubTotal
1	Servidor HP Proliant ML110 G4*	480 €	480 €
1	Sistema Operativo Debian	0 €	0 €
2	Horas de Técnico de Sistemas: - Instalación de la versión estable de debian. - Particionado de disco. - Selección de paquetes mínimos necesarios.	45 €	90 €
		TOTAL	570 €

* Donde hemos elegido un servidor con recursos más que suficientes para las tareas que va a desempeñar y con buena relación calidad/precio. Sus características técnicas son las siguientes:

Especificaciones de HP Proliant ML110 G4		
Procesador	Procesador Intel® Xeon® 3040 Dual-Core (1,86 GHz, FSB a 1066MHz, 1 x 2 MB de caché compartida de nivel 2); Procesador Intel® Pentium® D 915 (2,8 GHz, FSB a 800MHz, 2 x 2 MB de caché de nivel 2)	
Cache	1 x 2 MB de caché de nivel 2 compartida (modelos Xeon® 3040); 2 x 2 MB de caché de nivel 2 (modelos Pentium® D)	
Tipo de Memoria	512MB SDRAM PC2-5300 DDR2 sin memoria intermedia (667 MHz)	
Disco duro	Unidad SATA de 160 GB, 7.200 rpm y 1" (de serie en modelos SATA)	
Unidades ópticas	CD-ROM IDE (ATAPI) 48x	

Interfaz de red	Tarjeta de red Gigabit 10/100/1000 Broadcom 5721 (integrada)
Ranura de expansión	Dos ranuras de PCI de 32 bits/33MHz a 3,3 voltios; Dos ranuras PCI- Express (x4 y x8, ambas en un conector x8)
Dimensiones	17,5 x 42,6 x 36,7 cm
Peso	10,5 Kg
Garantía	La garantía limitada incluye 1 año en piezas, 1 año en mano de obra y 1 año de soporte en casa del cliente

PARTIDA 2. Sistema de acceso inalámbrico seguro: 802.1x			
Ud.	Concepto	Precio Unitario	SubTotal
1	Punto de Acceso inalámbrico*	50 €	50 €
2	Horas de Técnico de Sistemas: - Configuracion freeRADIUS - Configuracion punto de acceso 802.1x - Credenciales usuarios**	45 €	90 €
1	Horas de Formación a Usuarios: - Configuración de equipos cliente	35 €	35 €
		TOTAL	175 €

* El punto de acceso inalámbrico es el mismo modelo con el que trabajamos en nuestro banco de pruebas en el laboratorio, y que estudiamos en el capítulo sobre 802.1x. Adicionalmente, se podría ofrecer al cliente una gama completa de servicios basados en dispositivos inalámbricos: estudio de cobertura, instalación de puntos de acceso, certificado de emisiones electromagnéticas, etc..

** Suponemos un número de usuarios razonable para una oficina pequeña (10-30). No obstante, podría ampliarse este servicio (y sus relativos costes de ingeniería) ofreciendo la posibilidad de integración con un servidor LDAP.

PARTIDA 3. Configuración como router y otras funciones de red			
Ud.	Concepto	Precio Unitario	SubTotal
1	Tarjetas de Red Ethernet Gigabit PCI (10/100/1000)*	12 €	12 €
2	Horas de Técnico de Sistemas: - Análisis del direccionamiento de red - Configuracion de DHCP - Servidor Proxy DNS - Encaminamiento de paquetes - NAT	45 €	90 €
		TOTAL	102 €

* Tarjeta de red Ethernet adicional para nuestro dispositivo Debian, ya que inicialmente sólo viene con una interfaz de red.

PARTIDA 4. Configuración del cortafuegos			
Ud.	Concepto	Precio Unitario	SubTotal
1	Tarjetas de Red Ethernet Gigabit PCI (10/100/1000)*	12 €	12,00 €
1'5	Horas de Técnico de Sistemas: - Análisis de las necesidades del cliente - Configuración de reglas de filtrado	45 €	67,50 €
		TOTAL	79,50 €

* Tarjeta de red Ethernet adicional para nuestro dispositivo Debian, por si necesitamos tener una DMZ o zona desmilitarizada DMZ para ofrecer servicios al exterior.

PARTIDA 5. Detector de intrusos			
Ud.	Concepto	Precio Unitario	SubTotal
2	Horas de Técnico de Sistemas: - Análisis de las necesidades del cliente - Configuración de reglas de alertas/alarmas	45 €	90 €
		TOTAL	90 €

PARTIDA 6. Redes Privadas Virtuales			
Ud.	Concepto	Precio Unitario	SubTotal
2	Horas de Técnico de Sistemas: - Configuración de un túnel IPSEC punto a punto entre dos dispositivos.	45 €	90 €
2	Horas de Técnico de Sistemas: - Configuración de un servidor PPTP para dar acceso a usuarios remotos a nuestra red.	45 €	90 €
		TOTAL	180 €

PARTIDA 7. Mantenimiento y soporte		
Concepto		SubTotal
Incluye los siguientes servicios:* - Respuesta garantizada 48 horas (laborables) - Asistencia técnica de primer nivel en horario de oficina. - Gestión remota de incidencias.		
Linux sistema base		30 €
802.1x		30 €
Routing		20 €
Firewall		30 €
IDS		50 €
VPN		30 €
	TOTAL (mensual)	190 €

* Los servicios de mantenimiento y gestión de incidencias dependien de las partidas contratadas.

A continuación presentamos una tabla global que resume los precios totales de todas las partidas:

TOTALES	
Concepto	SubTotal (€)
Partida 1. Hardware e Instalación del sistema operativo Debian	570,00
Partida 2. Sistema de acceso inalámbrico seguro: 802.1x	175,00
Partida 3. Configuración como router y otras funciones de red	102,00
Partida 4. Configuración del Cortafuegos	79,50
Partida 5. Detector de Intrusos	90,00
Partida 6. Redes Privadas Virtuales	180,00
Partida 7. Mantenimiento y Soporte	190,00

A modo de ejemplo, obtener un dispositivo que implemente todas las tecnologías además de la contratación de todos los servicios de mantenimiento y soporte posibles tendría como importe: 1196,50 € (MIL CIENTO NOVENTA Y SEIS EUROS CON CINCUENTA CENTIMOS) más 190,00 € (CIENTO NOVENTA EUROS) mensuales en conceptos de mantenimiento.

4. CONCLUSIONES

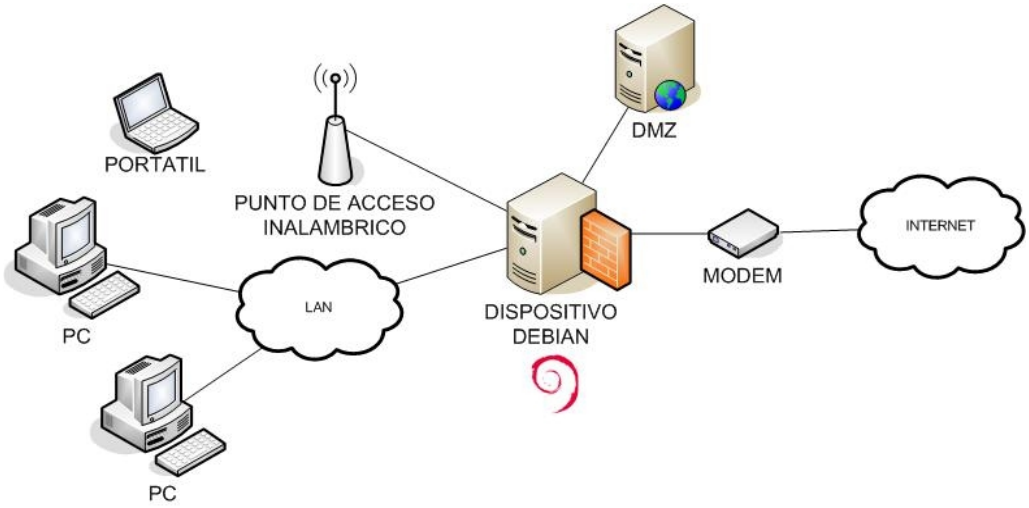
4. RESUMEN

4.1 Resumen y Cumplimiento de objetivos

Con todo el trabajo realizado anteriormente, nos hemos quedado con un dispositivo que es capaz de realizar las siguientes funciones:

- Autenticar usuarios de la red de área local inalámbrica (WLAN)
- Encaminar tráfico IP
- Compartir una conexión de área extensa (WAN) entre varios equipos de una red de área local (LAN)
- Permitir tráfico desde el exterior a los servidores ubicados en la zona desmilitarizada (DMZ)
- Filtrar paquetes
- Realizar túneles con redes privadas virtuales (VPN)
- Detectar intrusiones

El esquema de conectividad que hemos tenido durante todo el transcurso del trabajo ha sido tal el siguiente:



La máquina de nuestro dispositivo Debian es un PC antiguo con las siguientes características:

Pentium II 128 Mb RAM 350 Mhz

El sistema de archivos ha quedado como:

S.ficheros	Bloques de 1K	Usado	Dispon	Uso%	Montado en
/dev/hdc1	184M	64M	111M	37%	/
tmpfs	63M	0	63M	0%	/dev/shm
/dev/hdc9	1,3G	9,9M	1,3G	1%	/home
/dev/hdc8	111M	4,1M	101M	4%	/tmp
/dev/hdc5	1,4G	881M	456M	66%	/usr
/dev/hdc6	603M	392M	179M	69%	/var

Analizamos en esta sección el grado de cumplimiento de los objetivos planteados para el presente proyecto:

- En primer lugar necesitábamos instalar una versión estable del sistema operativo GNU/Linux en nuestra máquina prototipo. Realizamos, por tanto, una introducción al sistema operativo GNU/Linux, analizando las ventajas y desventajas respecto a otros sistemas operativos y su facilidad para entender y comunicarse con otras máquinas utilizando el protocolo TCP/IP. Después comentamos las características de las distintas distribuciones GNU/Linux existentes, sus versiones y entornos de uso comunes. Tras este análisis nos centramos en la distribución Debian y justificamos el porqué de utilizar esta distribución para nuestro proyecto. Continuamos el análisis descargándonos de Internet e instalando paso a paso la última versión estable de Debian en el momento de redacción del presente documento. Finalmente dimos una pincelada de cómo instalar nuevos paquetes y programas en Debian haciendo uso del comando apt-get, así como la utilización de algunas herramientas del sistema para eliminar aquellos paquetes que no necesitamos tras la instalación del sistema base con el objetivo de ir construyendo un dispositivo lo más compacto posible.

- Una vez instalado el sistema operativo comenzamos a analizar los procesos, recursos, aplicaciones y funcionalidades del núcleo para conseguir realizar las tareas de seguridad que nos propusimos en la parte introductoria del proyecto. Desarrollamos este análisis desde abajo hacia arriba en el modelo de referencia de capas OSI (Open System Interconnection); es decir, empezando desde la capa 1 o capa física viendo cómo está cableado el dispositivo, conectividad de los enlaces, después la conmutación a nivel de enlace, etc... Por tanto, comenzamos haciendo una introducción teórica de los dispositivos físicos de red a la vez que veíamos cómo administrar dichos dispositivos desde Debian. Describimos también el estándar 802.3 ethernet y el 802.11, siendo éste el de las redes inalámbricas WiFi.

Parte importante de nuestro proyecto fue el estudio de cómo brindar protección en las conexiones inalámbricas de los equipos que estuviesen presentes en nuestra red interna o red de área local. Para ello analizamos las deficiencias de los métodos de encriptación WEP y WPA e hicimos una justificación de la utilización del estándar de seguridad 802.1x. Nos paramos en ese momento también a ver cómo configurar un cliente inalámbrico que utiliza un sistema operativo Linux, configuramos el driver de la tarjeta inálambrica con ndiswraper y su configuración de red.

Por último, describimos en detalle el protocolo de seguridad 802.1x, viendo que era necesario la necesidad de utilizar algún tipo de servidor de autenticación de usuarios, como RADIUS (Remote Authentication Dial-In User Server); buscamos su implementación en GNU/Linux y la respuesta fue: FreeRadius. Lo instalamos sobre nuestra máquina Debian, describimos brevemente su funcionamiento y efectuamos una batería de pruebas de conectividad y autenticación con un PC actuando de cliente tanto en el sistema operativo Windows como en GNU/Linux.

- Después de haber estudiado el nivel 2 pasamos a estudiar servicios relacionados con el direccionamiento IP. Hicimos un repaso teórico sobre direcciones IP, máscaras, elementos básicos de red, formato del paquete TCP/IP y después pasamos a ver cómo configurar diversos parámetros de la capa de red en Linux, así como herramientas básicas de configuración.

En primer lugar, queríamos que nuestro dispositivo configurase de manera automática todos los parámetros de red de los equipos de nuestro sistema. Para ello analizamos el protocolo DHCP (Dynamic Host Configuration Protocol) e instalamos un servidor de DHCP en nuestro dispositivo.

Otra característica que nos interesaba era utilizar nuestra máquina como servidor DNS (Domain Name System); es decir, que resolviera las peticiones de traducción de nombres de dominio por direcciones IP a los clientes de la LAN. Instalamos pdnsd que es un proxy dns caché, es decir, que además de resolver la dirección haciendo uso de los recursos DNS de Internet, cada vez que una dirección fuera solicitada, sólo lo haría una vez y el resto se serviría desde el disco duro de nuestra máquina Debian.
Una vez llegados hasta aquí, configuramos nuestro dispositivo para que actuase como encaminador o router, permitiendo el paso de paquetes desde nuestra red local a Internet, función que realiza Linux en el propio Kernel. Después configuramos nuestro dispositivo para que hiciese traducción de direcciones de red o NAT, y así pudiera compartir una conexión a Internet entre varios ordenadores.

– Conseguido el hito anterior, nuestro dispositivo se comportaba como encaminador de red, ahora el objetivo era dotar de seguridad a esas comunicaciones IP, empezando por realizar filtrados de paquetes a distintos niveles. Para ello analizamos en detalle el módulo netfilter y la herramienta iptables para configurar reglas de filtrado. Utilizándola fuimos insertando reglas en nuestro firewall para proteger todas las comunicaciones inseguras. También citamos algunas herramientas para depurar el funcionamiento de nuestro firewall así como detectar vulnerabilidades.

Por otro lado, pusimos las bases de cómo detectar ataques de red de intrusos en nuestra máquina Debian comentando las herramientas existentes en Linux para realizar este tipo de tareas.

Respecto a túneles VPN, realizamos un repaso a los protocolos más comúnmente utilizados y a sus respectivas implementaciones en Linux, realizando dos pruebas de simulación con nuestra máquina Debian y otro PC corriendo en Linux: una de establecimiento de un túnel punto a punto entre ambas con el protocolo IPSec, y otra donde nuestra máquina Debian actuaba como servidor de VPN con protocolo PPTP.

Por último, para terminar con la seguridad, instalamos y utilizamos la herramienta SSH (Secure Shell) para administrar nuestra máquina remotamente de forma segura.

Así pues, con todo el trabajo anterior basándonos en el sistema operativo libre GNU/Linux, hemos convertido un viejo PC en un poderoso router multifunción, 100% configurable, pudiéndose ser amoldado a nuestras necesidades. Como justificamos en la introducción, debido a su flexibilidad y economía, es una buena alternativa para utilizar en un ambiente doméstico o pequeña empresa frente a cualquier dispositivo router comercial basado en sistemas propietarios, los cuales algunos de ellos necesitan licencias que se renuevan periódicamente para garantizar la máxima seguridad en todo momento. Paradójicamente, muchos de estos routers comerciales están también construidos internamente con sistemas operativos GNU/Linux.

4.2 Ampliaciones y trabajos futuros

Hay varias cosas que se han planteado para realizar en un futuro y ampliar la capacidad e inteligencia de nuestro dispositivo Debian. Se mencionan a continuación especificando brevemente ciertos detalles de su posible implementación:

– Se podrían implementar mecanismos para el balanceo de carga del tráfico que va dirigido hacia los servidores de la DMZ, esto nos permitiría tener máquinas redundantes y repartir el trabajo uniformemente sobre ellas. Uno de los principales problemas de los mayores sitios web en Internet es cómo gestionar las solicitudes de un gran número de usuarios. Se trata de un problema de escalabilidad que surge con el continuo crecimiento del número de usuarios.
Hay balanceadores de carga tipo round-robin (uno a uno) y por pesos (que son capaces de saber cual de los nodos está más libre y lanzarle la petición) el más conocido es LVS, sin embargo hay otros muy buenos como el Red-Hat Piranha, que no es más que un front-end de configuración de LVS. El LVS está en el cluster suite de Red Hat, pero también se puede instalar en Debian.

– Implementación de IPv6 (también llamada la Internet de nueva generación). IPv6 está destinado a sustituir el estándar IPv4, cuyo límite en el número de direcciones de red admisibles está empezando a restringir el crecimiento de Internet y su uso, especialmente en China, India y otros países asiáticos densamente poblados. Pero el nuevo estándar mejorará el servicio globalmente; por ejemplo, proporcionando a futuras celdas telefónicas y dispositivos móviles con sus direcciones propias y permanentes. A día de hoy se calcula que las dos terceras partes de las direcciones que ofrece IPv4 ya están asignadas.
Para habilitar IPv6 en nuestra máquina GNU/Linux tendríamos que recompilar el kernel dando soporte para Ipv6, aunque viene por defecto, también es interesante activar iptables para IPv6, para poder ampliar nuestro cortafuegos y filtrar tráfico Ipv6.

– Implementar mecanismos de calidad de servicio (QoS) para dotar de mayor prioridad a algún determinado tipo de tráfico sobre otro de menor imporancia. El kernel de Linux gestiona la forma en que los paquetes de datos son enviados por la red, de esta manera, podríamos modificar dicho comportamiento basado en colas para asignar prioridades a las distintas aplicaciones críticas sobre las que no se necesitan bajo retardo.

- Realización de pruebas de carga para sondear el rendimiento del sistema con un determinado hardware. Para simular cargas altas se pueden utilizar generadores de tráfico o emuladores de red.

- Filtrado de contenidos WEB. Utilizando un Proxy WEB como SQUID y herramientas asociadas se plantea la posibilidad de que nuestro dispositivo permita bloquear el contenido no deseado de páginas WEB a los ordenadores de nuestra LAN, restringiendo el acceso a páginas de entretenimiento, compras, páginas de chat entre otras.

- Desarrollo o instalación de alguna herramienta de gestión de red utilizando el protocolo SNMP, de tal forma que desde un cuadro de mandos podamos controlar el dispositivo remotamente y seamos capaces de obtener y aplicar configuraciones, recoger estadísticas de tráfico, gestionar inventarios, realizar informes, etc.

- Instalación o desarrollo de un interfaz gráfico de gestión similar a Webmin. Con él sería posible crear una aplicación basada en WEB que permitiese realizar las tareas del operador gráficamente, de forma remota y utilizando un navegador estándar. Esto permitiría que el operador no tuviese que utilizar el interfaz de comandos del sistema y limitaría al mínimo la formación requerida para la realización de sus tareas.

- Creación de una distribución de Linux (o distro) que nos permita instalar fácilmente el sistema operativo y todas las aplicaciones necesarias para construir nuestro dispositivo. Podría utilizarse para ello el proyecto metadistros, que son un conjunto de herramientas que nos permiten crear nuestro CD-Live desde una distribución cualquiera (Debian en nuestro caso) instalada desde 0, con los programas que queramos .

- Construcción de un sistema embebido. Un sistema embebido es un ordenador que a diferencia de un ordenador personal (PC) carece de teclado y pantalla en la mayoría de los casos. Dicho de otra manera, un sistema embebido consiste en una electrónica programable especialmente diseñada para soluciones específicas. De esta manera tendríamos nuestro sistema operativo Debian funcionando en perfectas condiciones en un dispositivo compacto, de reducidas dimensiones y bajo coste.

5. BIBLIOGRAFÍA Y REFERENCIAS

BIBLIOGRAFÍA

Enlaces de Internet sobre Aspectos Generales de GNU/LINUX

[1] ina Página WEB del Proyecto Debian: http://www.debian.org/

[2] The Linux Kernel Archives: http://www.kernel.org

[3] Definición de Debian en Wikipedia: http://es.wikipedia.org/wiki/Debian
[Fecha de extracción de la información: Julio 2007]

[4] La mayor comunidad de Debian en español: http://www.esdebian.org/

[5] Comunidad de Software Libre y Hardware abierto Utpinux: http://www.utpinux.org/

[6] Usuarios de GNU/Linux de Balears: http://www.bulma.net/
[Consulta de artículos publicados entre 2003-2006]

[7] Hispalinux, asociación de usuarios españoles de GNU/Linux: http://www.hispalinux.es/

[8] Linux Man Pages Online: http://man.he.net/

[9] El software como servicio: http://sinetgy.org/~jgb/articulos/software-servicio/
[Artículo de Barrapunto. Octubre 2002]

[10] Artículo: ¿De qué vive el software libre?
http://spanish.martinvarsavsky.net/tecnologaa-e-internet/ade-qua-vive-el-software-libre.html
[Autor: Martin Varsavsky. Abril 2007]

[11] Guía de compilación del kernel: http://www.frikis.org/staticpages/index.php/kernel
[Artículo de frikis.org. Marzo 2006]

[12] Recursos didáctivo on-line: Compilación del kernel paso a paso:
http://www.wikilearning.com/compilacion_del_kernel_paso_a_paso-wkc-876.htm
[Wikilearning. Febrero 2005]

Libros Técnicos

[13] Administración de sistemas Linux
[Autor: Dee Ann LeBlanc – Editorial: Anaya Multimedia. 2003]

[14] Redes Linux con TCP/IP – Guía avanzada
[Autor: Pat Eyler – Editorial: Prentice Hall. 2001]

[15] Linux Firewalls
[Autor: Robert L. Ziegler. Editorial: New Riders. 2002]

[16] Cisco Certified Network Associate. CCNA 1 y 2
[Cisco Press. 2005]

[17] Materiales didácticos on-line: Curso Linux Básico y Avanzado
[Antora. Centros de Innovación y Formación]

[18] Materiales didácticos on-line: Administrador de Redes bajo Linux
[Diasoft Formación]

[19] Intrusion Detection Systems with Snort.
Advanced IDS Techniques using Snort, Apache, Mysql, pHp and ACID.
[Prentice Hall. Rafee Ur Rehman]

[20] Snort for Dummies
[Wiley Publilshing, Inc. Charlie Scott, Paul Wolfe, Bert Hayes 2004]

Enlaces sobre Redes Inalámbricas en Linux

[21] Tecnologías WiFi en Wikipedia: http://es.wikipedia.org/wiki/Wi-Fi
[Fecha de extracción de la información: Febrero 2007]

[22] Configurar dispositivos WiFi en Linux: http://www.omerique.net/twiki/bin/view/TIC/WiFi
[Autor: Ricardo de los Santos. Febrero 2007]

[23] Artículo sobre seguridad Wi-Fi, WEP, WPA y WPA2.
www.hsc.fr/ressources/articles/hakin9_wifi/hakin9_wifi_ES.pdf
[Autor: Guillaume Lehembre. www.hackin9.org. 2006]

[24] Guía de Redes Inalámbricas con EAP-TLS y PEAP:
http://dns.bdat.net/wireless_eap_tls/book1.html
[Autor: Pedro Pablo Fábrega Martínez. Información extraída en Febrero.2007]

[25] Certificados Digitales: http://dns.bdat.net/wireless_eap_tls/x47.html
[Información extraída en Febrero 2007]

[26] Servidor RADIUS: http://felipe-alfaro.org/blog/category/radius/
[Información extraída en Febrero 2007]

[27] Seguridad en redes inalámbricas: http://dns.bdat.net/seguridad_en_redes_inalambricas/x80.html
[Información extraída en Febrero 2007]

[28] Más información sobre certificados digitales:
http://dns.bdat.net/documentos/certificados_digitales/c29.html
[Información extraída en Febrero 2007]

Enlaces sobre Administración de la Red en GNU/Linux

[29] Direcciones IP: http://es.wikipedia.org/wiki/Direcci%C3%B3n_IP
[Información extraída en Marzo 2007]

[30] Configuración de la red en Debian:
http://www.debian.org/doc/manuals/reference/ch-gateway.es.html
[Guía de Referencia de Debian]

[31] NAT (Dirección de traducciones de red)
http://es.wikipedia.org/wiki/Network_Address_Translation
[Información extraída en Marzo 2007]

[32] DHCP: http://es.wikipedia.org/wiki/DHCP
[Información extraída en Marzo 2007]

[33] Documentación sobre pdnsd: http://www.phys.uu.nl/~rombouts/pdnsd/doc.html
[Autor: Thomas Moestl y Paul Rombouts. Septiembre 2006.]

[34] Guía de Bulma sobre enrutamiento de paquetes:
http://bulma.net/impresion.phtml?nIdNoticia=1441
[Celso González. Agosto 2002]

[35] Netfilter, Firewalling, NAT and packet mangling for Linux: http://www.netfilter.org/documentation/

[36] Pequeño tutorial sobre Tcpdump: http://www.arrakis.es/~terron/tcpdump.html

Enlaces sobre IPtables

[37] Iptables Tutorial 1.2.2: http://iptables-tutorial.frozentux.net/iptables-tutorial.html
[Autor: Oskar Andreasson. 2006]

[38] Iptables basics: http://www.justlinux.com/nhf/Security/IPtables_Basics.html
[Autor: Prince Kenshi.]

[39] Filtering Packets with iptables:
http://www.unixreview.com/documents/s=1237/urm0103c/0103c.htm
[Autor: Joe “Zonker” Brockmeier. 2001]

[40] Artículo sobre Iptables y Masquerading:
– http://www.davidcoulson.net/writing/lxf/38/iptables.pdf
http://www.davidcoulson.net/writing/lxf/39/iptables.pdf
[Autor: David Coulson. Publicado en LinuxPro. Marzo 2003]

[41] Netfilter Tutorial: http://www.crhalpin.org/project/netfilter.html
[Información extraída en Marzo 2007]

[42] Manual Práctico de Iptables (1.2): http://www.pello.info/filez/firewall/iptables.html
[Autor: Pello Xabier Altadill. Información extraída en Marzo 2007]

Enlaces sobre Seguridad de Redes

[43] Definición de DMZ: http://es.wikipedia.org/wiki/DMZ

[44] Guía de Ubuntu para instalar un servidor SSH:
http://www.guia-ubuntu.org/index.php?title=Servidor_ssh
[Información extraída en Abril 2007]

[45] Redireccionar puertos con Iptables y NAT: http://bulma.net/body.phtml?nIdNoticia=1522
[Autor: Ricardo Galli Granada. 2003]

[46] Sistema de detección de intrusos:
http://es.wikipedia.org/wiki/Detecci%C3%B3n_de_intrusos
[Información extraída en Abril 2007]

[47] Red Privada Virtual: http://es.wikipedia.org/wiki/Red_privada_virtual
[Información extraída en Abril 2007]

[48] Introducción a las redes privadas virtuales sobre Linux:
http://www.lugro.org.ar/biblioteca/articulos/vpn_intro/vpn_intro.html
[Autor: Ramiro J. Caire. Información extraída en Abril 2007]

[49] Uso de OpenVPN en Slackware Linux: http://tuxjm.net/docs/openvpn-como4slack/
[Autor: Jorge Armando Medina. 2006]

[50] Información teórica sobre el protocolo IPSEC: http://www.ipsec-howto.org/spanish/x161.html
[Información extraída en Abril 2007]

[51] Using a Linux L2TP/IPsec VPN Server: http://www.jacco2.dds.nl/networking/freeswan-l2tp.html
[Enero. 2007]

[52] Debian IPSec Micro How-to: http://www.fukt.bth.se/~teddy/debian-ipsec
[Mayo 2006]

[53] IPSEC using Linux Kernel 2.6. http://shorewall.net/IPSEC-2.6.html
[Autor: Thomas M. Eastep. 2006]

[54] How to easily build a VPN with KAME IPSec Kernel 2.6:
http://users.cjb.net/ipsec/index.en_us.html
[Autor: Cristiano da Cunha Duarte. 2005]

[55] Linux 2.6 IPSec VPNs: http://www.sherman.ca/archives/2004/11/21/linux-26-ipsec-vpns/
[Autor: Frank Herbert.]

[56] The PPTP Server for Linux: http://www.poptop.org/

[57] Linux Freeswan: http://www.freeswan.org/

[58] PPTP Client for Linux: http://pptpclient.sourceforge.net/

[59] Información sobre Secure Shell http://es.tldp.org/Tutoriales/doc-ssh-intro/intro-ssh/node8.html
[Autor: Sebastian Gurin. 03-08-2006]

[60] Uso básico de ssh-agent: http://laespiral.org/recetas/1-100/receta66.html
[Autor: David Suela. 13-09-2001]

Enlaces sobre Distribuciones de Linux que implementan un Router / Firewall:

[61] Clarkconnect Server and Gateway: http://www.clarkconnect.com/

[62] Zebra, Free Routing Software distributed under GNU General Public License: http://www.zebra.org/

[63] NetBoz Firewall: http://www.netboz.net/

[64] Coyote Linux: http://www.coyotelinux.com/

[65] Minidistribuciones Linux: http://es.wikipedia.org/wiki/Minidistribuciones_de_GNU/Linux