

# TRABAJO DE DIPLOMA

*Proyecto de perfeccionamiento  
de la red informática y sus servicios  
en el Instituto Cubano de la Música.*

**Autor:** Gerson Ramírez Pedret

**Tutor:** Lic. Yuri Quintana

**Cotutores:** Ing. Raquel Stone Espinosa

Lic. Gerardo Damián Iglesias Rodríguez

**Instituto Cubano de la Música**

INSTITUTO CUBANO DE LA MUSICA



**Universidad de la Habana**

UNIVERSIDAD DE LA HABANA

**matcom**  
FACULTAD DE MATEMÁTICA Y COMPUTACIÓN

Tesis en opción al grado de Licenciado en Ciencias de la Computación.

**Ciudad de la Habana, 2008**

## Dedicatoria

*A mis padres*

*A mi novia*

*Al resto de mi familia*

*A mis amigos*

*A mis colegas*

## Agradecimientos

*Ante todo doy gracias a DIOS por haber removido todos aquellos obstáculos que habían impedido durante algún tiempo el desarrollo de este trabajo, y me acompañó en cada instante de su confección.*

*Agradezco asimismo a mis padres José Felipe y Aracelis y a mi novia Brenda por la mucha cooperación y paciencia que me dedicaron durante todo este tiempo.*

*Otro tanto a mi tutor Yuri y cotutores Raquel y Gerardo que me fueron de gran ayuda y sin ellos no hubiese sido posible la satisfactoria culminación de este empeño.*

*Al Dr. Jesús Salomón, quien tan atentamente me ayudó en la primera etapa a organizar mis ideas y estructurar este contenido.*

*En especial al colectivo de trabajadores del Instituto Cubano de la Música, por las facilidades que pusieron a mi disposición.*

*A mi familia por darme aliento y depositar su confianza en este logro.*

*A la comunidad de usuarios y desarrolladores BSD.*

*Y a todos aquellos que no menciono, pero que también pusieron su grano de arena.*

*“Un producto reemplaza a otro si el mismo ofrece a los clientes un incentivo para el cambio que tenga más peso que el costo del cambio o que se sobreponga a la resistencia impuesta por el cambio.*

*El producto reemplazo ofrece un incentivo para el cambio si con respeto a su precio, el mismo ofrece a los clientes una mayor utilidad que el producto que se usaba anteriormente.”*

*M.E. Porter.*

# Indice

Indice .....	iv
Introducción .....	<b>¡Error! Marcador no definido.</b>
Problema.....	vii
Capítulo I Estado Actual. ....	1
1.1.    Marco del proyecto.....	2
1.2.    Descripción de la topología de la red actual.....	3
1.2.1.    Necesidad de modificar en la topología actual.....	5
1.2.2.    Necesidad de inversión de tecnología de red.....	6
1.3.    Plataformas de Sistemas de la red actual.....	6
1.3.1.    Necesidad de inversión en servidores profesionales. ....	7
1.3.2.    Migración al Software Libre.....	8
Capítulo II nálisis y rediseño de la topología. ....	11
2.1.    Presentación de la nueva topología. ....	12
2.1.1.    Características de las topologías de cortafuegos. ....	13
2.2.    Selección del cortafuegos y host bastión.....	14
2.2.1.    Análisis del hardware. ....	15
2.2.2.    Presentación de pfSense. ....	17
2.2.3.    Propuesta de implementación del cortafuegos. ....	20
2.2.3.1.    Instalación y configuración básica de pfSense. ....	20
2.2.3.2.    Aislamiento físico y lógico de las subredes.....	26
2.2.3.2.1.    Esquema de direccionamiento IP. ....	27
2.2.3.3.    Creación de la subred DMZ.....	32
2.2.3.3.1.    Topología de la DMZ. ....	32
2.2.3.3.2.    Configuración de la DMZ en pfSense. ....	34
2.2.3.4.    Configuración de la subred LAN. ....	37
2.2.3.5.    Configuración de la subred WLAN.....	40
2.2.3.5.1.    Configuración del punto de acceso.....	40
2.2.3.5.2.    Portal Cautivo. ....	45
2.2.3.6.    Concepción de la subred RAN. ....	46
2.2.3.6.1.    Conectividad mediante enlaces arrendados.....	47
2.2.3.6.2.    Accesos desde la WAN por VPN. ....	49
2.2.3.7.    Mecanismos de seguridad de red en pfSense. ....	50
2.2.3.7.1.    Las reglas del cortafuegos. ....	50
2.2.3.7.2.    Acceso desde la DMZ a la Internet. ....	54
2.2.3.7.3.    Acceso al exterior desde las redes internas. ....	54
2.2.4.    Otras prestaciones de pfSense. ....	58
2.2.4.1.    Alta disponibilidad y salva de la configuración. ....	58
2.2.4.2.    Publicación de servicios de redes internas. ....	60
2.2.4.3.    Otros proxies de aplicación. ....	61
2.2.4.4.    Registro de sucesos.....	62
2.2.4.5.    Monitorización. ....	62

Capítulo III uía de migración al software libre de los servicios de red.....	65
3.1. Significado de la migración al software libre en el ICM.....	66
3.2. Selección de los sistemas operativos libres.....	67
3.2.1. Caracterización general de los BSD.....	68
3.2.1.1. ¿Qué es BSD?.....	68
3.2.1.2. Un poco de historia.....	68
3.2.1.3. Tipos de BSD.....	69
3.2.1.4. ¿Por qué los BSD no se conocen mejor?.....	70
3.2.2. Presentación de FreeBSD.....	71
3.2.2.1. FreeBSD y los sistemas operativos libres.....	72
3.2.2.2. FreeBSD y la seguridad.....	75
3.2.2.3. Casos de uso de FreeBSD.....	76
3.2.2.4. Ventajas en la adopción de soluciones FreeBSD.....	77
3.3. Migración de los servidores de producción de la DMZ.....	78
3.3.1. Selección del hardware.....	79
3.3.2. Implementación de los servidores.....	79
3.3.2.1. Instalación básica de FreeBSD.....	80
3.3.2.2. Servidores DNS del dominio <i>icm.cu</i> .....	84
3.3.2.3. Servidor Web, FTP y Bases de datos.....	88
3.3.2.3.1. Instalación y configuración del servidor Web.....	89
3.3.2.3.2. Instalación y configuración del servidor FTP.....	92
3.3.2.3.3. Instalación del servidor de Bases de Datos.....	94
3.3.2.4. Servidor de correo corporativo.....	96
3.3.2.4.1. Selección de un MTA libre.....	97
3.3.2.4.2. Sistema de administración de dominios virtuales.....	98
3.3.2.4.3. Acceso de clientes, POP3, IMAP y corporativos.....	105
3.3.2.4.4. Acceso al correo desde la web.....	108
3.4. Migración de los servidores de la red interna.....	111
3.4.1. Administración de redes mediante dominios.....	112
3.4.2. Gestión web de la Intranet.....	114
3.4.2.1. Gestores de Contenidos Web.....	114
3.4.3. Servidor Proxy.....	116
3.4.3.1. Análisis de Hardware.....	117
3.4.3.2. Instalación y configuración de un servidor proxy.....	117
3.4.3.2.1. Configuración de jerárquica de proxies.....	119
3.4.3.2.2. Control de acceso y autenticación.....	119
3.4.3.2.3. Generación y análisis de trazas.....	121
3.4.3.2.4. Monitoreo y control restricciones.....	123
3.4.4. Servidor de almacenamiento y salva.....	123
3.4.4.1. Presentación de FreeNAS.....	124
3.4.4.2. Selección del Hardware.....	127
Conclusiones.....	128
Recomendaciones .....	129
Bibliografía.....	130
Anexos.....	130

## Introducción

Justo ahora recuerdo aquellos días, cuando de pequeño solía visitar el trabajo de mi padre, en aquellos tiempos CAC, ahora CENSAI. Fue justo allí mi primer encuentro con lo que ahora significa mi carrera y mi vida, “computación”, palabra cuyos significados para mí se tornan indescriptibles. Desde aquel instante mi atracción por ese mundo fue en constante ascenso, interés bonificado en todas las etapas de mi vida de estudiante, primaria, secundaria y preuniversitario, donde al terminar fueron justo los estudiantes de esta facultad de Matemática y Computación, que hoy me ve graduarme, los que me abrieron las puerta del gran salón “Ciencias de la Computación”. Desde ese instante comenzaron a desentrañarse ante mí, progresivamente, todos aquellos que hasta ese momento representaban misterios de una gran caja negra. Aquello no sólo me permitió entender, me permitió comenzar a crear. En los inicios de la carrera mi vocación, dentro de todo aquel mundo, se tornaba difusa. Expuso mis potencialidades ante varias temáticas y me sentí a gusto, pero no fue hasta cuarto año donde me sentí especialmente atraído por la asignatura de redes, que me dio una pista sólida de hacia donde debería dirigir mis esfuerzos.

En Julio de 2006 empiezo a trabajar como instructor de informática en un Joven Club, donde pude dar mis primeros pasos como administrador de red en una pequeña red local y poner a prueba muchos de los conocimientos teóricos que había obtenido durante la carrera. Mi interés y desenvolvimiento en la temática me permitieron integrar las filas del primer grupo de certificación de redes promovido por el Ministerio de las Comunicaciones y la Informática en colaboración con el gobierno de la India. Aquel curso contribuyó a consolidar un tanto más mis conocimientos de administración de sistemas y redes, conocimientos que me permiten en Julio de 2007, ocupar un cargo como administrador de red en el nodo nacional de la red de cultura, fue allí templada mi formación, estaban allí ante mí las líneas a seguir y las metas a alcanzar, la administración de redes y sistemas operativos implementados con software libre. Tras un plazo de formación, fui llamado a ocupar un cargo similar, esta vez en una institución de cultura, el Instituto Cubano de la Música, al tiempo de que fui invitado a participar en un curso de superación, cuyo propósito consistía en fomentar la política de migración al software libre en todas las instituciones patrocinadas por el Ministerio de Cultura.

Al llegar al Instituto encuentro diezmadas las capacidades informáticas y los servicios de red del Centro, motivado fundamentalmente por deficiencias técnicas y conceptuales. Rápidamente me di a la tarea de conciliar con los directivos la posibilidad de mejorar las prestaciones informáticas haciendo una evaluación justa de los requerimientos que esta misión implicaba. Al mismo tiempo comencé a valorar la posibilidad de incorporar en las soluciones los conocimientos acumulados sobre software libre y sistemas operativos gratuitos como GNU/Linux y FreeBSD, y de ese modo dar cumplimiento también a la política de migración del Ministerio de Cultura. Fue justamente ese el nacimiento de este proyecto, acometer seriamente la tarea a fin de encontrar respuestas para aquel conjunto de deficiencias y en la evaluación de soluciones considerar con prioridad las que se correspondía con una proceso de migración de los servidores y servicios de red al software libre, y así cumplimentar una etapa lógica y fundamental del proceso total de migración.

Durante el periodo de estudio de requerimientos iniciales se incorpora al Centro el actual Jefe de Departamento de Informática y uno de los cotutores asistenciales de esta tesis, quien le dio un gran impulso a todo este proyecto, pues su experiencia en la materia me permitió concebir de forma organizada todo el proceso de perfeccionamiento de la red y los servicios informáticos del Instituto Cubano de la Música. Este proyecto consta de tres secciones, en las que se abordan diferentes temáticas, pero todas cooperan íntegramente en un proyecto único de perfeccionamiento de red. Se analiza el escenario inicial, se proponen esquemas de soluciones a las deficiencias y se traza una tentativa guía de migración al software libre que propone estimulantes alternativas a los sistemas privativos en uso, al tiempo de que contribuye con el movimiento migracional nacional, pudiendo repercutir en diferentes niveles, a nivel del Centro, a nivel del Ministerio y a nivel de país.

## *Problema*

Hacer propuestas de ajustes en la arquitectura y funcionamiento de la red del Instituto Cubano de la Música a fin de erradicar el conjunto de deficiencias y limitaciones actuales.

Proponer alternativas de solución con el objetivo de brindar nuevos servicios de red y de conectividad beneficiando al Centro y al conjunto de instituciones de la música patrocinadas por el ICM.

Proponer un proceso organizado de migración al software libre, mostrando las cualidades de la familia de sistemas BSD como opción de plataformas de sistemas de servidores de producción y de servicios.

## *Objetivos*

- Conformar una propuesta de rediseño de la red informática con carácter fiable que, además de mejorar la prestación de los servicios actuales, sirva de infraestructura tecnológica para incorporar un nuevo conjunto de prestaciones informáticas en el Instituto Cubano de la Música y su sistema de instituciones.
- Hacer, en cada momento, un análisis de requerimientos e inversiones que brinde un respaldo sólido tanto al nuevo rediseño de la red como al mejoramiento de los servicios y su disponibilidad en la misma, dicho análisis deberá abarcar la tecnología de red, la adquisición de nuevos servidores profesionales y el resto del material complementario como las fuentes de corriente ininterrumpidas y el equipamiento de preservación del clima.
- Elaborar una guía de migración al software libre que de soporte a las nuevas tecnologías informáticas de la red y los servicios del Instituto Cubano de la Música y su sistema de instituciones, y que represente documentación y cumplimiento de las políticas nacionales y ministeriales relacionadas con la tarea de migración.

# I

Estado Actual.

## 1.1. Marco del proyecto.

El Instituto Cubano de la Música es una entidad perteneciente al Ministerio de Cultura, cuya Dirección radica en Calle 15 No. 452 e/ E y F. Plaza de la Revolución, Ciudad de la Habana.



Fig. 1.1 Fachada frontal del Instituto Cubano de la Música.

El Instituto Cubano de la Música tiene como misión proponer, dirigir y controlar la aplicación de la política cultural en la rama de la música y los espectáculos en el país y garantizar el desarrollo, protección, enriquecimiento, defensa y promoción del patrimonio musical de la nación.

**Estructura de gestión de la actividad informática.**

En la entidad hay una Dirección Informática que se subordina al Vicepresidente de Relaciones Internacionales y al Vicepresidente Primero. Al frente de esta se halla un Dr. Ciencias Técnicas, cuenta con un técnico y tres especialistas. El técnico cumple la función de asistencia técnica, mantenimiento y reparaciones menores, un aspirante al cargo de especialista principal juega el rol de Administrador de la Red, un Lic. desempeña el cargo de Responsable de Seguridad Informática y una especialista se encarga de la sección de desarrollo de las aplicaciones, además se cuenta una adiestrada que trabaja en el desarrollo de software y asistencia técnica. En los subepígrafes que siguen se muestra la organización estructural que poseen las tecnologías informáticas que se relacionan con este proyecto, pues sientan el punto de partida.

## 1.2. Descripción de la topología de la red actual.

El Instituto Cubano de la Música consta de una Red Local con topología de estrella, que se encuentra desplegada con cable de par trenzado en los dos pisos del edificio, con un Servidor Controlador de Dominio sobre Windows 2003 Server, a la cual se enlazan en la actualidad un estimado de 80 estaciones de trabajo y laptops existentes. Este servidor trabaja con un Directorio Activo en Windows 2003 que rige la seguridad de autenticación en las estaciones de trabajo de la red del Instituto, el cual se utiliza igualmente de servidor de ficheros y salva. La organización del Directorio Activo le permite servir de DNS para las maquinas que pertenecen al Dominio. Además actúa como servidor de ficheros y salva, este servidor tiene un hardware adecuado para dicha prestación, pues en sus especificaciones técnicas muestran que es un servidor profesional optimizado para este tipo de desempeño, de hecho es el único servidor profesional con el que contaba el instituto antes de comenzar este proyecto y a pesar de ya no estar en las últimas tecnologías es digno de tener en cuenta para soluciones de red como servidor de ficheros y otros servicios ligeros.

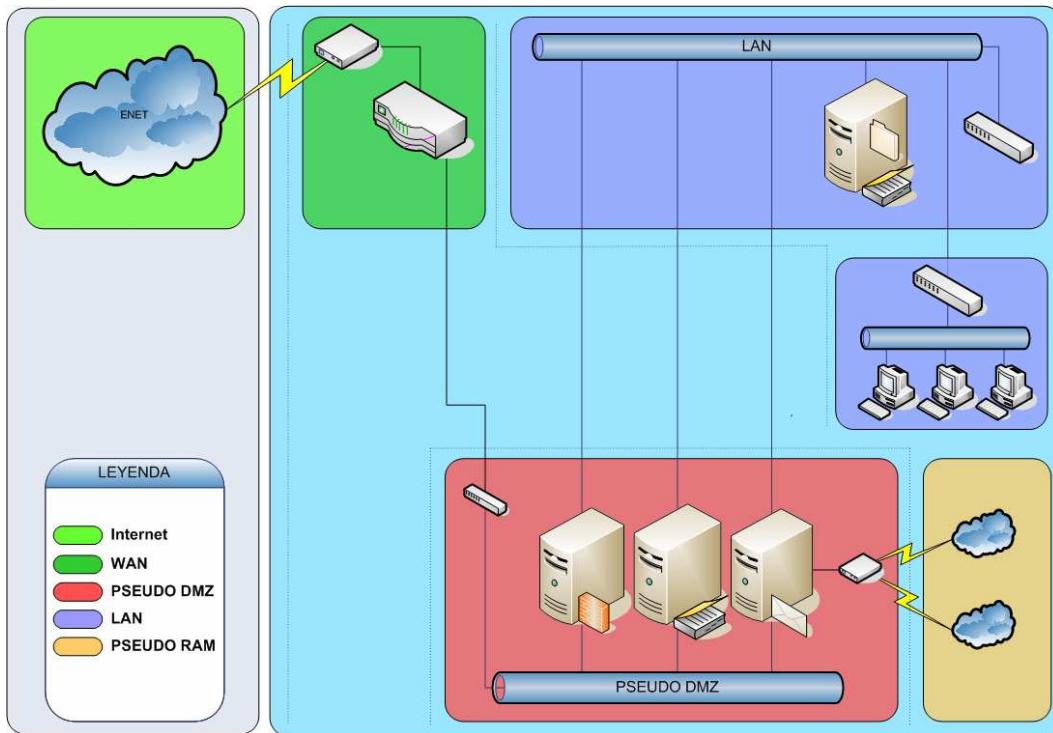


Fig. 1.2 Mapa topológico de la red informática del ICM.

La conexión a Internet se realiza mediante un enlace arrendado de 128 Kbps cuyo proveedor es Enet. Se cuenta para la conexión con un MODEM-ROUTER Telindus Crocus HS y un enrutador Cisco 2610MX.

El Instituto tiene asignadas 8 IP reales en el rango 200.55.136.168/29, donde se identifican cada uno de los servidores con las siguientes IP:

- IP 200.55.136.169: Identifica al Router Cisco 2610.
- IP 200.55.136.170: Identifica al ISA Server 2004.
- IP 200.55.136.172: Identifica al DNS **dnsicm.icm.cu**.
- IP 200.55.136.173: Identifica al Servidor de Correo **mailicm.icm.cu**

El otro servidor que se encuentra de cara a Internet es el Proxy el cual actúa, como su nombre lo indica, de servidor proxy y cortafuegos de la red interna, es este servidor el que mantiene todas las políticas de acceso a Internet de los usuarios y estaciones de trabajo del ICM. Este servidor desempeña esta función utilizando el ISAServer 2004, sistema que a pesar de sus dimensiones, es relativamente fácil de configurar y mantener, prestando además un excelente servicio estadístico y de logs, generando reportes con información relevante.

Otra importante tarea que se lleva a cabo a través del servicio de acceso a la web es la actualización del antivirus desde Internet. Está claro que esta tarea se ejecuta del mismo modo que se utiliza la navegación por parte de los usuarios, pero no deja de ser importante destacarla, pues una red, donde el 100% de sus estaciones de trabajo utilizan Windows como sistema operativo, sin un antivirus potente y bien actualizado, colapsaría en un corto plazo de tiempo.

El instituto cuenta con un dominio corporativo de correos **icm.cu**. El correo internamente se gestiona con *Mdaemon 9.0* sobre Windows 2003 Server. Este servidor brinda a las redes internas otras prestaciones como los protocolos de clientes de correos como el POP3, el IMAP y el acceso vía web mediante el cliente web de correos *WordClient*. A este servidor acceden (por un MODEM que tiene conectado) mediante conexión de acceso telefónico dos instituciones que hacen uso del correo corporativo, las mismas tienen reservado su un dominio personalizado para sus respectivos buzones, por lo que descargan el correo con cuentas multipop y se les permita el envío haciendo SMTP relay en nuestro servidor.

### 1.2.1. Necesidad de modificar en la topología actual.

La topología de red actualmente concebida incumple un sinnúmero de patrones conceptuales y tecnológicos que irrumpen en la semántica de redes. Esta cuestión hace imposible su categorización como una red eficiente y segura, o sea una red fiable. Además carece de soporte para las nuevas pretensiones que se imponen en los servicios de red del instituto. A grandes rasgos se han identificado las principales carencias y necesidades que se han tomado en cuenta como pautas iniciales en el desarrollo de este proyecto:

- La necesidad de establecer comunicación entre la red actual del instituto y la red de área local que soportará los servicios informáticos de las oficinas alojadas en un local aledaño al centro, actualmente en remodelación. Se valora la posibilidad de hacer esto de forma transparente, de modo que estas dos redes locales queden fusionadas en una sola red local de mayores dimensiones permitiendo la centralización de la administración, la aplicación de las políticas de seguridad y acceso a los servicios recursos y servicios.
- La necesidad de la delimitación entre redes internas y red externa, y los tipos de interacciones que habrán entre estas. En esta decisión influyen cuestiones de seguridad, organización, disponibilidad, entre otras.
- La necesidad de delimitar un backbone que soporte altas tasas de transferencias, es importante recalcar que en el instituto se manipula y se almacenan volúmenes de información relevantes, los que en ocasiones se hace necesario mover dentro de la red por diferentes razones.
- La necesidad de crear una infraestructura tecnológica que permita brindar servicios de conectividad a instituciones dependientes del centro.
- La necesidad de establecer enlaces múltiples con nuestra proveedora de servicios de Internet, con el objetivo de mejorar nuestros servicios de conectividad internos (ancho de banda), de las nuevas instituciones conectadas y la posibilidad futura de la delimitación de tráfico.
- La necesidad de brindar soporte de conectividad de red inalámbrica que pudiera beneficiar a los directivos del centro que, por las características de su trabajo, utilizan equipamiento portátil, en muchos de los casos con soporte de conectividad inalámbrica. Resulta, igualmente, muy útil en ocasiones donde se instalan en el centro puestos de mando, por eventos de distintas índoles para los cuales se habilitan ordenadores, con necesidad de conectividad, pues en el centro cuenta con tecnología portátil para este soporte.

### 1.2.2. Necesidad de inversión de tecnología de red.

Es posible deducir que la tecnología utilizada en la infraestructura informática actual no brinda soporte a prácticamente ninguna de las carencias latentes en las prestaciones de la red del Instituto. Indiscutiblemente el mejoramiento cualitativo de la conectividad y el ancho de banda trae como necesidad la inversión en tecnología de red actualizada con los estándares modernos.

Por solo citar ejemplos de las inversiones de tecnología y equipamiento de redes, tomamos las conexiones que se proyectan establecer con la edificación aledaña y las Instituciones de la Música. Para la primera será necesaria la adquisición de tecnología de fibra óptica pues sería esta la única manera en que cumpliría con las especificaciones del proyecto. Para el segundo caso será necesario conciliar enlaces arrendados con la empresa telefónica y de este modo enlazar las distintas instituciones. A lo largo de este proyecto se muestran otros ejemplos en los que se hacen necesarias inversiones.

### 1.3. Plataformas de Sistemas de la red actual.

A manera de resumen y para no pasarlo por alto se ha realizado un análisis de las plataformas de sistemas en los servidores de producción. Debe entenderse por plataforma la combinación hardware-sistema operativo-aplicaciones de servicios y por servidores de producción, los ordenadores que brindan el conjunto de servicios soportados sobre una red determinada. Es importante que las innovaciones que se hagan con el objetivo de mejorar y/o migrar la plataforma de los servicios, brinden, al menos, el conjunto de prestaciones que existen actualmente.

Teniendo en cuenta lo antes mencionado, a continuación mostramos una lista de los servidores de producción que se tendrán en cuenta:

- Servidor Proxy – Cortafuegos: ISASERVER
- Servidor DNS: DNSICM
- Servidor Correo – RAS: MAILSERVER
- Servidor Dominio Primario – Ficheros: ICMSERVER

Se ha resumido a manera de tabla los elementos más importantes:

NOMBRE PC	HARDWARE	SIST. OP	SERVIDORES	RENDIMIENTO
ICMSERVER	P3 a 1.6GHz, 2 procesadores 1GB RAM 2 HD 9GB, 1 HD 200GB	Windows Server 2003 Enterprise Edition	Active Directory, DNS (interno)	Regular (aislados desperfectos técnicos)
MAILSERVER	P4 1.80GHz 512MB RAM 1 HD 40GB	Windows Server 2003 Enterprise Edition	MDaemon 9.01 RAS Server	Bueno (reemplazado, desperfectos técnicos frecuentes)
ISASERVER	Celeron 2G 512MB RAM 1 HD 80GB	Windows Server 2003 Enterprise Edition	Isa Server 2004	Bueno (desperfectos en tarjetas de red)
DNSICM	P4 1.3GHz 256MB RAM 1 HD 8GB	Windows Server 2003 Enterprise Edition	DNS (externo) IIS MSSQL Apache MySQL	Excelente (No desperfectos técnicos de hardware)

Tabla 1.1 Resumen técnico de los servidores de la red.

A modo de complemento en la información de la tabla sólo resta apuntar que todos los servidores han presentado desperfectos técnicos de software (sistema operativo y servicios) necesitando reiniciar el equipo (en el mejor de los casos) y otros ajustes (reinstalaciones, etc.), sobre todo como resultado de las interrupciones de corriente. Se estima que la cota máxima de duración de encendido (uptime) no supera los 30 días en ninguno de los servidores, pues por motivos distintos se hace necesario reiniciarlos en cortos plazos de tiempo.

### 1.3.1. Necesidad de inversión en servidores profesionales.

Como se ha podido apreciar en el subepígrafe anterior, es un problema latente, la discontinuidad de los servicios, las que a menudo van acompañadas de desperfectos técnicos de hardware. Está más que claro que un hardware no profesional no es el apropiado para estos tipos de prestaciones.

Además, más adelante en este proyecto se muestra nuevos aportes a los servicios informáticos del instituto. Estos nuevos servicios imponen nuevos niveles de rendimiento y disponibilidad; pues se prevé depositar en los servidores del ICM la confianza sobre un conjunto creciente de prestaciones que van a implicar un consumo de recursos elevado comparado con los inicialmente evaluados. La disponibilidad y continuidad de los servicios son factores fundamentales en su fiabilidad.

En este proyecto se contemplan también otros factores como la preservación de un clima adecuado y el soporte de fuentes de corriente ininterrumpida. Teniendo esto en cuenta esto, como parte de las inversiones se valorarán la compra de un split de 1 tonelada y del mismo modo se patentá la idea de la adquisición de un grupo electrógeno automático que en conjunción con las fuentes de respaldo existentes puedan mantener una continuidad de servicios.

### 1.3.2. Migración al Software Libre.

Llegado este punto son notables muchas de las limitaciones que a simple vista (sin abundar, de entrada, en cuestiones filosóficas) reporta el uso de software privativo en el ICM, en el Ministerio de Cultura y en general en todo el país. Es un problema latente desde muchos ángulos y cada día que pasa se hace más imperiosa la necesidad de que, a conocimiento de causa, se le de un vuelco al modelo de software privativo aún vigente. En pos de ello ha surgido todo un movimiento mundial que le imprime un gran impulso a esta tarea, teniendo claro que son muchas y difíciles barreras las que hay que superar.

Teniendo en cuenta que proyectar este trabajo hacia un enfoque filosófico del software libre y la migración sería un tema recurrente y repetitivo, pues sobrada bibliografía [1a][1b][1c] respalda esta temática, será sólo abordado desde un punto de vista práctico, sólo haciendo énfasis en algunas salvedades que suelen general desconocimiento y confusión:

1. "**Software libre**" vs. "**GNU/Linux**": En la actualidad se tiende a confundir el término "**Software libre**" con el de "**GNU/Linux**". Eso es algo totalmente erróneo, "**GNU/Linux**" es una categoría de sistema operativo (entendamos sistema operativo como núcleo + componentes de software), donde se hace (en muy pocos casos) realidad la aplicación generalizada de las libertades que gozan los integrantes del "**Software libre**". "**Software libre**" va más allá, habla de filosofía, libertades (y hasta restricciones en algunos casos), pero donde quiera que exista software, puede existir software libre. Siempre y cuando un programa, una aplicación, un formato o norma de documento, una documentación, u otro componente de software, se rija bajo las libertades que está filosofía brinda, estaremos ante software libre, cualquiera sea el sistema operativo o la función del componente de software en cuestión.
2. "**Libertad**" vs. "**Libertad + restricción**": En ocasiones se suele abusar del término "**Libertad**", el software libre, a pesar de tener libertades, se "*cuida*" con "**restricciones**" (ej. copyleft) [A], pero... ¿Son deseables o necesarias esas "**restricciones**"?, ¿Acaso, no son las "**restricciones**"... ausencia de libertades? Esto es toda una temática polémica. Pero muy intencionalmente en esta tesis se da muestras de que una filosofía como la del software libre puede sobrevivir (y lo ha hecho desde mucho antes de que surgieran las modernas concepciones de software libre) sin las "**restricciones**" y muestra de ello es el modelo de licencias BSD bajo los que se desarrollan algunos de los productos que se exponen en este trabajo. Se dejan estos análisis a consideración del lector, pero se invita a usar los términos con fundamento y conocimiento de causa, pues solo así se podrá defender una filosofía.

3. "**Migración**" vs. "**Solución**": Una guía de migración no tiene que ser necesariamente absoluta (ni a GNU/Linux), cualquier parcialidad de una guía de migración al software libre introduce alternativas para sistemas propietarios y de este modo promueve el uso del software libre. Pero ciertamente la tarea es compleja, pues no se debe tomar a la ligera este proceso. Es recomendable dividir el proceso en etapas [B] y se deben fundamentar sólidamente cada una de las propuestas, demostrar que no solo son alternativas, sino que constituyen solución a problemas. Es necesario abstraerse del problema "*migración*" y enfocarse el problema "*solución*" y desde este punto hacer valoraciones de costos, jugar con todas las variables y no dejarse cegar por el término "*gratis*", pues este término en ocasiones suele ser relativo cuando además del precio del producto se implican otros costos.

### **¿Porqué migrar?**

Una vez que se han esclarecido (desde un enfoque crítico) algunos términos, se retoma la tarea. A continuación se exponen algunos elementos que apoyan el proceso de migración y estimulan a abandonar sistemas propietarios, en especial los sistemas operativos Windows de Microsoft.

- **Disminuir la dependencia a vendedores de código propietario:** Es común hacer dependencia de software propietario, puede suceder a la hora de las actualizaciones del producto, y a la larga supone un gasto de dinero innecesario. Las actualizaciones en el software libre, además de gratuitas, suelen ser más transparentes (menos protocolos) y más automatizadas (ej. Mozilla Firefox).
- **No hay necesidad de presupuestar el coste de software, mantenimiento y personal encargado:** Las licencias de software suponen un gasto adicional frente al salario del personal, además elevan el TCO (Total Cost of Ownership) de los equipos de cómputo. Todo esto puede ahorrarse para gastarlo en otros proyectos. En Cuba actualmente esto no es tan así, pero es sugerente estar preparados ante un eventual cambio.
- **Acceso a más herramientas:** El acceso a un número casi ilimitado de herramientas (desarrollo, oficina, web, seguridad, etc.), sin necesidad de solicitar permiso para obtenerlo debido a su coste o licencia de uso. En la medida en que se gane en cultura del software libre, no será necesario ya promover tráfico pirata de sistemas. Intercambiar software libre, en cualquiera de los modos de intercambio, será una tarea estimulante y contribuirá sin limitaciones al desarrollo tecnológico.
- **Probarlo antes de comprarlo:** Muchas empresas propietarias si ofrecen versiones de prueba o gratuitas para desarrollo (uso no comercial), en algunos (los peores) casos es imposible ver cómo funciona un producto antes de comprarlo. En el software libre esto no es así, los usuarios pueden usar el software al tiempo que disfrutan de sus libertades sin ningún coste el tiempo que necesiten probarlo, incluso pueden usarlo indefinidamente.
- **Soporte por parte de una comunidad de usuarios:** Algo que valoran mucho las empresas es el soporte oficial del software. En el software libre el soporte toma carácter comunitario y aunque se puede congeñar contratos de soporte y asesoría, en pocas ocasiones esto es en extremo necesario, pues se puede capacitar personal en la propia empresa no sólo en el uso del software, también en la gestión de soporte.

- **Acceso al código y la posibilidad de modificarlo según tus necesidades:** Esto reporta una gran ventaja, pues tener que esperar una nueva versión o tener que comprar una versión actualizada de un producto para conseguir una funcionalidad necesitada reporta un problema difícil de tratar. Si se dispone del código y del permiso de modificarlo la tarea se simplifica pues se puede adaptar el software para un uso exclusivo de un usuario o de una empresa.
- **No hay exceso de características inútiles:** En proyectos de software libre, las nuevas funcionalidades suelen venir dadas por las necesidades de los usuarios, no por las ideas de un departamento de desarrollo o marketing. Se ha puesto de moda también que las empresas les pagan a los desarrolladores por implementar funciones en un producto, el beneficio (por ser libre) no solo incide directamente en la empresa interesada, sino en toda la comunidad de uso.
- **Solución de errores y nuevas implementaciones con más rapidez:** en algunos casos los errores se solucionan mucho antes incluso de que lo detecten los usuarios.
- **Más seguridad:** algo que crea mucha controversia, pero algunos estudios reportan al software libre como más seguro. Pero algo que si es cierto es que los sistemas UNIX-like y el software libre en general son menos propensos a virus y ataques de seguridad. Existen considerables diferencias en los modelos de acceso de los usuarios entre los sistemas Windows y los sistemas descendientes de UNIX, donde para hacer daño son necesarios privilegios de administración, privilegios a los que se acceden explícitamente, al contrario de los sistemas Windows.
- **Estabilidad de los sistemas:** por supuesto, ningún sistema operativo es perfecto y es fácil poner en duda la veracidad de planteamientos de usuarios que argumentan no haber tenido nunca un fallo de un sistema operativo. Sin embargo, algunos sistemas operativos pueden ser muy estables, incluso después de varios años de funcionamiento. Esto es más cierto en plataformas de servidores con algunos sistemas libres como GNU/Linux y los BSD. Cuando un sistema falla, hay que apagar o reiniciar, por lo tanto, si el equipo puede permanecer en marcha y funcionando correctamente durante mucho tiempo, entonces se puede decir que el sistema es estable.

# II

Análisis y rediseño de la topología.

## 2.1. Presentación de la nueva topología.

Los factores expuestos en el Capítulo 1 hacen necesario un rediseño de la topología previa, con el objetivo de incorporar los nuevos elementos y prestaciones. Se ha mantenido el modelo de estrella, pero se han procurado un conjunto de conceptos diferentes niveles de ausencia en la red concebida anteriormente.

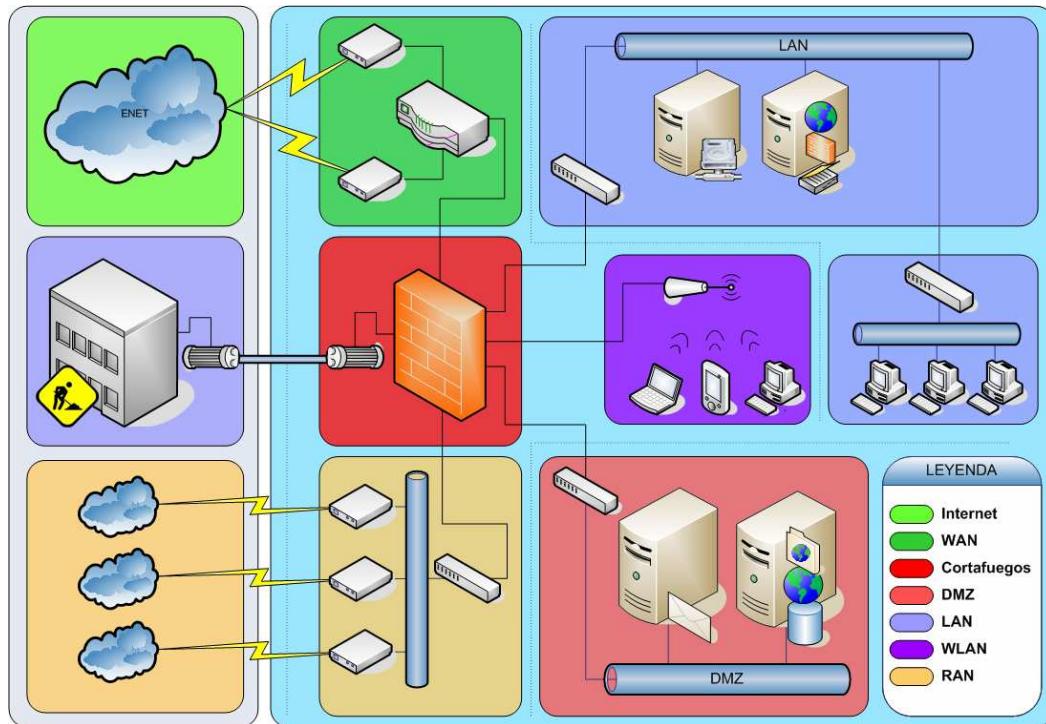


Fig. 2.1 Rediseño topológico propuesto para la red informática del ICM.

Se tuvo en cuenta un amplio número de factores, a continuación se muestran los parámetros básicos:

1. En el rediseño de la topología se han tenido en cuenta, con una propuesta de solución a cada uno de los requisitos y necesidades que se mencionan en el Capítulo 1.
2. La topología resultante del rediseño es compatible con la topología actual en un alto porcentaje. La mayoría de los cambios añadidos en la topología inicial hacen que sea más:
  - a. *Flexible*, la red empresarial quedará dividida en subredes físicas y lógicas:
    - i. Carácter modular e independencia en el funcionamiento en sectores físicos de red, en caso de avería se puede aislar el sector, para que no se vea afectada el resto de la red.
    - ii. Futuros cambios resultarán menos traumáticos, fundamentalmente a los usuarios finales de la red.

- b. *Extensible y escalable*, elementos de extensibilidad han sido incorporados:
  - i. Mecanismos para integración mediante conectividad de las instituciones de la Música.
  - ii. Incorporación de tecnología inalámbrica.
  - iii. El factor modularidad incrementa la escalabilidad, pues un aumento futuro en la complejidad de la red no repercute sobre las subredes existentes.
- c. *Segura*, enfocada fundamentalmente en el incremento de la seguridad:
  - i. Modelo de cortafuegos, red perimetral y proxies de aplicación.
  - ii. Aislamiento de subredes.
  - iii. Aplicación de los controles de acceso.
- d. *Robusta*, la implementación del diseño se ha concebido bajo criterios de alta disponibilidad y tolerancia a fallos:
  - i. Las modificaciones más críticas han sido concebidas transparentemente, posibilitando una rápida reconfiguración en vistas a mantener en todo momento la conectividad.
  - ii. Brecha abierta a la implantación de un cluster de cortafuegos de alta disponibilidad.

### 2.1.1. Características de las topologías de cortafuegos.

Existen varios modelos en la protección de redes internas, algunos muy sencillos que ni siquiera incluyen la definición de la red perimetral. Los diseños están fundamentados por tres decisiones [C] básicas:

1. La primera de ellas, la más importante, hace referencia a la política de seguridad de la organización propietaria de la red a proteger. Evidentemente, la configuración y el nivel de seguridad potencial será distinto en una empresa que utilice un cortafuegos para bloquear todo el tráfico externo hacia el dominio de su propiedad (excepto, quizás, las consultas a su página web), frente a otra donde sólo se intente evitar que los usuarios internos pierdan el tiempo en la red, bloqueando por ejemplo todos los servicios de salida al exterior excepto el correo electrónico. Sobre esta decisión influyen, aparte de motivos de seguridad, motivos administrativos de cada organismo.
2. La segunda decisión de diseño a tener en cuenta es el de monitorización, redundancia y control deseado en la organización. Una vez definida la política a seguir, hay que definir cómo implementarla en el cortafuegos indicando básicamente qué se va a permitir y qué se va a denegar. Para esto existen dos aproximaciones generales: o bien se adopta una postura restrictiva (denegamos todo lo que explícitamente no se permita) o bien una permisiva (permitimos todo excepto lo explícitamente negado); evidentemente es la primera la más recomendable de cara a la seguridad, pero no siempre es aplicable debido a factores no técnicos sino humanos (esto es, los usuarios y sus protestas por no poder ejecutar tal o cual aplicación a través del cortafuegos).

3. Por último, la tercera decisión a la hora de instalar un red con cortafuego recae en el plano económico: en función del valor estimado de lo que deseemos proteger, debemos gastar más o menos dinero, o no gastar nada. Un cortafuegos puede no entrañar gastos extras para la organización, o suponer un desembolso de considerables sumas de dinero: seguramente un departamento o laboratorio con pocos equipos en su interior puede utilizar un PC con Linux, Solaris o FreeBSD a modo de cortafuegos, sin gastarse nada en él; pero esta aproximación evidentemente no funciona cuando el sistema a proteger es una red de tamaño considerable; en este caso se pueden utilizar sistemas propietarios, que suelen ser caros, o aprovechar los enrutadores de salida de la red, algo más barato pero que requiere más tiempo de configuración que los cortafuegos sobre Unix en PC. De cualquier forma, no es recomendable a la hora de evaluar el dinero a invertir en el cortafuegos fijarse sólo en el coste de su instalación y puesta a punto, sino también en el de su mantenimiento.

## 2.2. Selección del cortafuegos y host bastión.

Un **cortafuegos** (*firewall*), es un elemento de hardware o software utilizado en una red<sup>1</sup> de computadoras para controlar las comunicaciones, permitiéndolas o prohibiéndolas según las políticas de red que haya definido la organización responsable de la red. Su modo de funcionar es indicado por la recomendación RFC 2979, que define las características de comportamiento y requerimientos de interoperabilidad. La ubicación habitual de un cortafuegos es el punto de conexión de la red interna de la organización con la red exterior, que normalmente es Internet; de este modo se protege la red interna de intentos de acceso no autorizados desde Internet, que puedan aprovechar vulnerabilidades de los sistemas de la red interna. Un cortafuegos correctamente configurado añade protección a una instalación informática, pero en ningún caso debe considerarse como suficiente. La seguridad informática abarca más ámbitos y más niveles de trabajo y protección.

Los cortafuegos están a menudo conformados por dos módulos lógicos, el cortafuegos de capa de red o de filtrado de paquetes (obligatorio) que funciona a nivel de red (capa 3 del modelo OSI, capa 2 de la pila de protocolos TCP/IP) como filtro de paquetes IP. A este nivel se pueden realizar filtros según los distintos campos de los paquetes IP: dirección IP origen, dirección IP destino. A menudo en este tipo de cortafuegos se permiten filtrados según campos de nivel de transporte (capa 3 TCP/IP, capa 4 Modelo OSI) como el puerto origen y destino, o a nivel de enlace de datos (NO existe en TCP/IP, capa 2 Modelo OSI) como la dirección MAC. Un segundo modulo el cortafuegos de capa de aplicación (opcional, pero necesario). Trabaja en el nivel de aplicación (nivel 7) de manera que los filtrados se pueden adaptar a características propias de los protocolos de este nivel. Por ejemplo, si se trata de tráfico HTTP se pueden realizar filtrados según la URL a la que se está intentando acceder. Un cortafuegos a nivel 7 de tráfico HTTP es normalmente denominado proxy y permite que las computadoras de una organización entren a Internet de una forma controlada.

---

<sup>1</sup> Este tipo de modelo donde el host bastión es, a su vez, el cortafuegos centralizado se conoce como cortafuegos de red, pues existen aplicaciones que realizan tareas similares en los host conocidas como cortafuegos de host.

Existen cortafuegos implementados en hardware y en software. Los cortafuegos por hardware son equipos dedicados profesionales que realizan funciones tanto de enrutamiento como de filtrado de paquetes. Los más sencillos implementan sólo el primer módulo, mientras que otros más sofisticados hacen el trabajo completo. Su rendimiento y aplicación se corresponden con sus elevados costes. Generalmente se utilizan en grandes y complicadas infraestructuras de redes. El mercado de estos dispositivos está liderado por la Cisco Systems y sus renombrados exponentes los Cisco PIX.

Por otro lado tenemos los cortafuegos por software, los que son adaptables a diferentes arquitecturas de hardware no dedicado. En la actualidad tenemos implementaciones de estos sistemas compatibles con toda la diversidad de sistemas operativos, tenemos ejemplos, ipTable (Linux) y pf (OpenBSD y BSDs en general) y otras implementaciones para Windows, que se integran como cortafuegos de host, o sea, instalados en computadoras comunes y servidores de producción de propósito general. Además se han creado distribuciones Linux y BSD dedicadas, enfocadas fundamentalmente al reaprovechamiento de hardware en desuso (la mayoría son compatibles con hardware moderno), y otros como ISA Server que se integra en ediciones Windows de servidores convirtiéndola en servidores de seguridad dedicado. En este campo tenemos ejemplares tanto gratuitos como de coste (ISA Server y Otros).

Se ha hecho un estudio de varios de estos cortafuegos. Como punto de partida, se ha utilizado un artículo [2a] donde se hace una comparación entre varias de las distribuciones de cortafuegos gratuitas, sin descartar otras opciones [2b] que se pudieran llegar a considerar. Las opciones de cortafuegos por hardware han sido desechadas por sus altos costes al igual que las soluciones no gratuitas de código cerrado pues no cumplen con las políticas de migración al software libre. Finalmente se ha decidido usar pfSense, una distribución cortafuegos basada en FreeBSD.

### 2.2.1. Análisis del hardware.

El host bastión estará ubicado en el centro (**Fig. 2.1**) de la red. Esto es significativamente importante pues es un elemento a tener en cuenta, tanto para la selección del hardware que dará soporte a la PC cortafuegos, como en el software que realizará esta tarea.

Entre los elementos que intervienen en el análisis de hardware, basándonos en el diseño adoptado está la necesidad de que el equipo posea al menos 6 interfaces de red, una para cada subred a conectar, de preferencia algunas de ellas a 1Gb/s, fundamentalmente las que van conectadas al backbone [3] de la red interna, esto unido al enlace de banda ancha mediante fibra óptica con la edificación adyacente, permitiría conseguir el propósito de elevar el ancho de banda del backbone (ahora extendido). Los enlaces a Internet, en cambio, no necesitan esta tecnología, pues una tarjeta de 100 Mb/s daría más que a baxto para los enlaces que a lo sumo puede llegar a unos pocos Mb/s y eso en un caso muy optimista y contando con una considerable suma monetaria.

La PC del cortafuegos para dar soporte a la modalidad instalada de pfSense sugiere un disco rígido u algún dispositivo de almacenamiento flash, pues de esta manera se puede luego, como veremos más adelante, añadir paquetes como Snort, Squid, Radius, etc.

El hardware más sugerente para este tipo de servidor pudiera estar entre los equipos miniPC, equipos basados en una sola placa que utilizan un hardware de tamaño reducido, integrable en el armario de comunicaciones además de no requerir protección con un SAI de apagado y puesta en marcha automático, ya que no están basados en disco duros rígidos.

Ejemplo de estos dispositivos son los miniPC FabiaTech, en particular modelo FX5622. El equipo tiene 8 puertos de red, de los cuales 4 Ethernet de 100 Mbit/s y 4 de FastEthernet de 1 Gbit/s. Puede incorporar un disco duro de 2,5" y/o una Compact Flash (que puede actuar también como disco duro). En el **Anexo II.A** se muestra la ficha técnica de este dispositivo.

Sin embargo, procede crear una solución alternativa, con recursos quizás más accesibles, que aunque no sea óptima, de solución factible dentro del marco de posibilidades y en un plazo apropiado. A pesar de que la dirección del centro ha depositado todo el apoyo para este proyecto, especialmente en lo que a inversiones se refiere, aspectos técnicos como este van más allá de la inversión.

### Soluciones alternativas

Encontrar un hardware apropiado solo consistiría encontrar una PC que de algún modo soporte la instalación de 6 tarjetas de red, como ejemplo de este tipo de placas base se cuenta con la Asus CUV4X-DLS que dispone de una interfaz de red instalada de fábrica (*onboard*) y 5 slots de expansión en los que se podrían habilitar el mismo número de tarjetas de red, con diferentes interfaces de cableado y soporte de anchos de banda, incluso tarjetas de múltiples puertos (existen hasta de 4 puertos y son muy útiles para el ahorro de slots de expansión). En el **Anexo II.B** se pueden observar muestras de algunos de estas tarjetas con sus respectivos datos técnicos.

La variante de utilizar dos cortafuegos en serie (con hardware más modesto) dividiendo las tareas de control de tráfico sería posible, pero ciertamente esto implicaría trabajo extra en la configuración de dos cortafuegos en lugar de uno.

Y una última y quizás la más práctica y apropiada, a falta de otros recursos, sea que, mediante la adquisición de un conmutador (switch) de última generación con soporte para VLAN, utilizar el soporte que brinda pfSense para esta tecnología, siempre y cuando lo soporten también las tarjetas de red en el cortafuegos, cosa que es ya muy común en las tarjetas de red modernas. De este modo se pueden optimizar, en cuanto a cantidad, el uso de las tarjetas de red, que es donde radican fundamentalmente las deficiencias de los hardware no profesionales.

Las VLAN [4], o redes virtuales, se usan para dividir segmentos de red a nivel de conmutadores. Básicamente, se asigna un identificador de VLAN a cada puerto del conmutador, de manera que todos los puertos que tienen el mismo identificador actúan como si estuvieran conectados a un mismo conmutador (sin VLAN). Además cada puerto puede estar conectado a varias VLAN, incluso todas. En estos casos, son llamados puertos troncales (trunk) ya que suelen ser utilizados para interconectar conmutadores.

Esta última opción tiene otras ventajas, pues muchos de estos tipos de conmutadores implementan tecnología de enrutamiento y filtrado de nivel 3, como muchos enruteadores, y lo que es particularmente beneficioso en el caso de nuestro centro, algunos o todos los puertos son de 1Gb/s, esto nos puede también ayudar a alcanzar la meta de incrementar en ancho de banda del backbone de la red interna y de la DMZ, ya que combinando la tecnología VLAN con soporte de ancho de banda, se puede lograr beneficiar las dos o más subredes en un único conmutador. En el **Anexo II.C** se referencia un ejemplo de este tipo de equipamiento ofertado por comercializadores nacionales.

## 2.2.2. Presentación de pfSense.

pfSense [5] es una poderosa y estable solución bajo licencia BSD, por tanto de libre distribución, que nos permite expandir nuestras redes sin comprometer su seguridad. Es una distribución dedicada que hace de enruteador y cortafuegos. Su desarrollo comenzó en el 2004, como descendiente directo de la también prestigiosa distribución dedicada m0n0wall basada en FreeBSD, un proyecto de seguridad de redes enfocado principalmente a los sistemas embebidos o empotrados. Las razones por las cuales no se ha elegido m0n0wall en nuestro caso de estudio pueden verse claramente en una [D] de las secciones del manual de usuario de m0n0wall, lo que entra en contraste con nuestras intenciones, como veremos más adelante.

En la actualidad pfSense es usado para proteger redes de todos los tamaños, desde las caseras hasta gigantescas empresas y se han obtenido reportes de sistemas pfSense trabajando con miles de máquinas detrás del cortafuegos. Con pfSense se pueden mantener varias subredes separadas una de las otras simplemente añadiendo reglas en el cortafuegos, identificadas por diferentes funciones en su desempeño, dándole a cada una adecuada configuración de los accesos.

Tiene una comunidad de desarrollo muy activa, de ahí que en cada versión, en particular las estables, incorpore muchas funciones nuevas orientadas principalmente a la flexibilidad, escalabilidad y por supuesto a la seguridad.

El cortafuegos forma parte de Kernel del sistema, de hecho, se trata del Packet Filter (PF) originario de OpenBSD, quien está actualmente nominado como el sistema operativo más seguro del mundo.

Los desarrolladores escogieron FreeBSD en lugar de OpenBSD por su facilidad de instalación en el mundo de las PCs y debido a que ya existía BSD Installer [6], una versión muy, muy reducida de FreeBSD, además de que en los desarrolladores de la familia de sistemas BSD existe un gran concepto de cooperación y la mayoría de las aplicaciones se diseñan con vistas y facilidades para ser portadas hacia el resto de dichos sistemas.

La distribución viene en una imagen de CD que apenas alcanza los 100 MB, que puede ser igualmente utilizada como live-CD, de esta forma será enteramente funcional ejecutándose en la RAM y permitirá probar la compatibilidad del hardware. Además se puede instalar en el disco duro y en memoria flash. Existe también una edición para sistemas empotrados de dispositivos dedicados que optimizan los accesos a discos, preservando la vida de las memorias ROM [7] de estos dispositivos.

En pfSense, casi toda la administración de los servicios puede ser llevada a cabo mediante una interfaz web, que contiene todos los componentes de configuración. Una vez arrancado el sistema, se puede acceder a la misma desde una máquina conectada en la misma red que el cortafuegos utilizando un navegador web. Inicialmente es cargado un multiformulario (wizard) que nos lleva por toda la configuración. Toda la configuración hecha en la interfaz web se mantiene íntegra en un archivo de configuración, pfSense brinda mecanismos para pasar este fichero a soportes magnéticos (floppy), en caso de fallo se puede restablecer una configuración desde uno de estos ficheros. En el caso de la versión instalada la configuración permanece en el disco duro o memoria flash según sea el caso.

pfSense ya viene listo para añadirle un conjunto de estas aplicaciones pertinentemente preparadas que puedes ser instaladas y configuradas de la propia interfaz Web algunas de las más útiles pueden ser Snort, MRTG, Radius y proxies. Una vez que se tenga pfSense instalado se puede acceder a las mismas mediante la interfaz Web, lo que permitirá que sean instaladas directamente desde la misma con un simple click, pero es también posible instalarlas utilizando la consola de comandos (shell) como se ha hecho en FreeBSD por años. Es este otra de las ventajas que tiene trabajar, con esta distribución, ya que para usuarios avanzados, por ejemplo administradores de red con experiencia en el trabajo con los sistemas UNIX-like, pueden incorporarse aplicaciones extras en el sistema del repositorio de FreeBSD. Por supuesto esto último puede tener implicaciones directas tanto en el rendimiento como en la seguridad, por lo que es necesario estar bien seguro de lo que se está haciendo, pero está claro que puede ser muy útil incorporarle aplicaciones con otras funciones. A pesar de que los paquetes de FreeBSD distribuidos por la FreeBSD.org no son oficialmente soportados por pfSense, siempre se pueden lograr las soluciones deseadas con una pequeña carga de esfuerzo extra.

Una de las grandes limitantes que presenta un administrador a la hora de decidirse por pfSense es la escasez de documentación. pfSense es una distribución muy joven y sus primeras versiones no difieren mucho de su progenitor (m0n0wall), pero se mantiene evolucionando constantemente y ganando en aceptación, es por ello que muchos autores individuales, fundamentalmente administradores, han escrito guías y manuales más o menos detallados de usos específicos de pfSense. El proyecto no cuenta aún con una guía de usuario, aunque noticias recientes (a la fecha de desarrollo de este proyecto) se refieren a la confección de la guía oficial y de un libro sobre administración del sistema que probablemente estén listos para dar soporte a la versión RELEASE de la rama 2.0. Por el momento contamos con guías individuales públicas, el manual de usuario de m0n0wall (útil aún en la configuración de pfSense) y las listas y foros de discusión.

pfSense incluye todas las características de los cortafuegos comerciales incluso cortafuegos por hardware profesionales. A continuación se muestra el conjunto de características que convierten a pfSense en el cortafuegos indicado para este proyecto.

## Cortafuegos básico

- Filtrado por IP, protocolo y puertos para el tráfico TCP y UDP en origen y destino.
- Permite limitar conexiones simultáneas a base de reglas.
- Permite hacer filtrado avanzado por sistemas operativos.
- Sistema de trazas habilitado en las reglas que se procesan.
- Política de rutas muy flexible.
- Permite el uso de alias para la identificación de grupos de IPs, redes y puertos. Esto hace que el conjunto de reglas se mantenga limpio y fácil de entender, especialmente en entornos con múltiples IP públicas y numerosos servidores.
- Capacidad para hacer cortafuegos transparente de layer 2 – haciendo puente entre las interfaces y filtrando el tráfico entre ellas.
- Puede ser apagado el filtro y ser solo usado como enrutador. Esto permite enlazar todas las redes primeramente para luego activar el filtrado y configurar poco a poco las reglas.

## Características avanzadas

- DHCP, servidor DHCP y agente de relevo DHCP.
- Ajuste de tráfico. Esto permite darle prioridades a los tipos de tráfico, por ejemplo se le puede subir la prioridad al tráfico de VOIP o bajar la prioridad al tráfico de las redes p2p, mensajería instantánea o ftp para que no afecte en la navegación.
- Balance de carga. Si se están ejecutando dos servidores de Web, se puede redirigir el tráfico al menos cargado o al que contiene el recurso solicitado. Es igualmente considerable el balance en los servidores de correo. Esto previene contra la sobrecarga de los servidores.
- Captive Portal [8] Permite controlar el acceso a Internet. Esto es muy útil en los entornos donde se brinda acceso inalámbrico libremente y otros donde se desea un nivel extra de seguridad en el acceso a Internet.
- Monitoreo y Reportes. Gráficos RRD que mantiene información histórica de distintos elementos que puede ser visualizada en forma de reportes en la interfaz Web, como por ejemplo: utilización de la CPU, estados del cortafuegos, monitoreo de flujo total, monitoreo de flujo por interfaces, promedio de paquetes por segundo por cada interfaz, tiempos de respuestas de ping hechos a interfaces WAN, colas del regulador de tráfico, entre otros.
- VPN<sup>2</sup>, soporte para redes privadas virtuales mediante el uso del Protocolo de Seguridad de Internet (IPSec), OpenVPN, o PPTP.

<sup>2</sup> En las versiones 1.2.X esta y otra características avanzadas tienen algunas limitaciones, que han sido ya erradicadas en las versiones en desarrollo de la 2.0, cuya liberación está planificada para fines del 2008 o principios del 2009 (previo al momento de la puesta en práctica de esta guía).

- Aplicaciones y componentes extras. Pueden ser instalados otros servicios como:
  - Snort, sistema ligero de detección de intrusos.
  - Squid, Proxy caché de alto rendimiento.
  - FreeRadius, implementación gratuita del protocolo RADIUS.
  - IMSpector, proxy para mensajería instantánea con capacidades para el control de acceso.
  - nmap, ntop, herramientas de auditoria, control de seguridad y rendimiento.
  - DNS servidor de nombres de dominio.
- Tablas de estado, la tabla de estados de un cortafuegos mantiene la información de las conexiones abiertas, pfSense es un cortafuegos de estados [9] gracias a pf [10], el cortafuegos de OpenBSD. Muchos tipos de cortafuegos carecen de esta habilidad lo que impide un control refinado del estado de las conexiones.
- Redundancia, dos o más cortafuegos pueden ser configurados como un grupo de recuperación ante fallas. Si en uno de ello falla alguna interfaz de red o es inhabilitado totalmente, el otro comienza a trabajar.
- Traducción de direcciones IP (NAT).
  - El redireccionamiento de puertos o rangos y el uso de múltiples IPs públicas.
  - 1:1 NAT para IPs individuales, incluso subredes completas.
  - NAT de Salida.
  - Configuración por defecto de todo el tráfico de salida por la IP de la WAN, en los casos de varias interfaces WAN, en la que será usada.
  - El NAT de salida avanzado permite deshabilitar el comportamiento por defecto, mediante la creación de reglas flexibles de NAT pertinentemente ajustadas, o el no uso de NAT.
  - NAT Reflection, quien permite que algunos servicios sean accedidos por IPs públicas desde redes internas al cortafuegos.

### 2.2.3. Propuesta de implementación del cortafuegos.

A lo largo de este subepígrafe se muestra de forma bastante práctica, muy cercana a lo que sería la implementación real del cortafuegos sobre pfSense en el entorno que nos ocupa. Aquí se muestran a tareas generales como la instalación de la distribución pfSense y la configuración de algunas de sus prestaciones.

#### 2.2.3.1. Instalación y configuración básica de pfSense.

La imagen (descargable desde el sitio de pfSense) es un live-CD por lo que será necesario para ejecutarlo configurar antes nuestro BIOS para que nos permita arrancar desde CD. Con este live-CD podemos probar la compatibilidad de nuestro hardware sin necesidad de instalarlo, incluso de reconocer todo el hardware satisfactoriamente tendremos, al ejecutarlo, un pfSense completamente funcional, ejecutándose en la RAM, que se puede configurar, salvando luego la configuración en un disquete o memoria flash; pero no es esta la modalidad que utilizaremos, en cambio utilizaremos la opción de instalación en disco duro.

Al arrancar la máquina con el live-CD podemos ver un conjunto de opciones y un contador inverso. Inmediatamente podemos seleccionar la opción 1, que es la opción por defecto, al instante nos mostrará las interfaces que reconoce con sus respectivas direcciones MAC para utilizarlas en la configuración inicial. Primero nos preguntará si estamos interesados en configurar la VLAN a lo que respondemos que no, para pasar a la configuración de las interfaces.

Es entonces cuando se seleccionan las interfaces que serán utilizadas para WAN y LAN respectivamente (**Fig. 2.2**). En principio, son las únicas interfaces que son necesarias para que funcione el cortafuegos. pfSense por su parte automáticamente le asigna la IP 192.168.1.1 a la interfaz LAN y configura con DHCP, de ser posible, la interfaz WAN, esto está orientado principalmente a aquellos que obtienen la dirección de su proveedor de servicios. Claro, es posible luego cambiar esta configuración por defecto en el entorno de configuración web que pone pfSense a la disposición de sus usuarios desde una PC en la red LAN.

```
Valid interfaces are:  
le0  00:0c:29:ff:4b:58  
le1  00:0c:29:ff:4b:62  
le2  00:0c:29:ff:4b:6c  
le3  00:0c:29:ff:4b:76  
  
Do you want to set up VLANs first?  
If you are not going to use VLANs, or only for optional interfaces, you should  
say no here and use the WebConfigurator to configure VLANs later, if required.  
  
Do you want to set up VLANs now [y:n]?n  
  
*NOTE*  pfSense requires *AT LEAST* 1 assigned interfaces to function.  
        If you do not have *AT LEAST* 1 interfaces you CANNOT continue.  
  
        If you do not have at least 1 *REAL* network interface cards  
        or one interface with multiple VLANs then pfSense  
        *WILL NOT* function correctly.  
  
If you do not know the names of your interfaces, you may choose to use  
auto-detection. In that case, disconnect all interfaces now before  
hitting 'a' to initiate auto detection.  
  
Enter the WAN interface name or 'a' for auto-detection: le0  
  
Enter the LAN interface name or 'a' for auto-detection  
(or nothing if finished): le1  
  
Enter the Optional 1 interface name or 'a' for auto-detection  
(or nothing if finished):  
The interfaces will be assigned as follows:  
  
LAN  ->le1  
WAN  ->le0  
  
Do you want to proceed [y:n]?■
```

Fig. 2.2 Proceso de inicio del sistema pfSense.

Seguidamente pfSense muestra un menú con varias opciones, este menú resultará muy familiar pues es el mecanismo de acceso y configuración básico que ofrece el sistema y es mostrado siempre que el sistema se inicia. Para acometer la tarea debe ser seleccionada la opción 99, por la cual se guía al usuario guiará por la instalación de pfSense en el disco duro (**Fig. 2.3**) mediante el BSD Installer que, mencionado anteriormente en la presentación de pfSense.

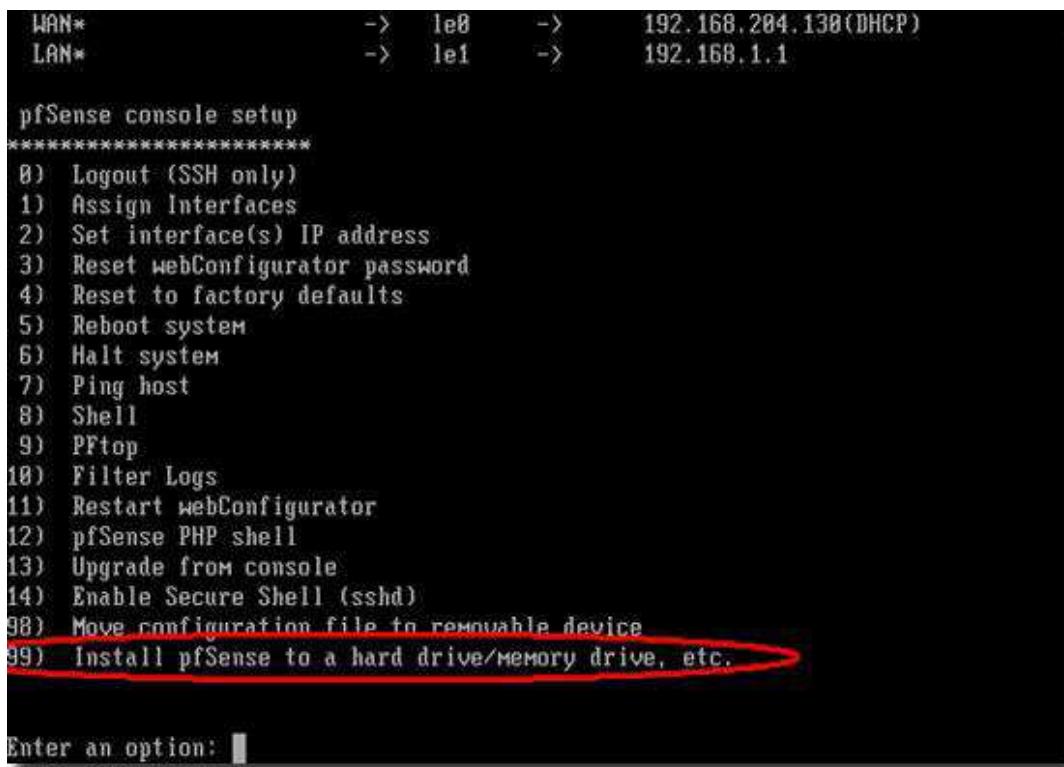


Fig. 2.3 Menú de consola de pfSense.

Se asume que esta PC solo tendrá pfSense instalado, por lo que la instalación puede tomar el disco completo, no será necesario un disco (memoria flash) de gran capacidad. Al terminar de instalarse en el disco duro pfSense se reinicia, será necesario retirar el CD del lector para que arranque utilizando el disco duro (es muy sugerente volver a cambiar la configuración de arranque del BIOS y por cuestiones de seguridad, y de ser posible restringir el acceso al BIOS con una contraseña). Finalmente carga el sistema, esta vez desde el disco duro, por lo que los cambios en la configuración quedarán residentes en el disco para posteriores reinicios.

### Configuración básica posinstalación.

Luego de que ha reiniciado el sistema se puede acceder al panel de configuración web desde alguna otra PC conectada en esta red. La dirección será <http://192.168.1.1>. Al acceder vía web es necesario autenticarse, el usuario y la contraseña por defecto son **admin** y **pfsense** respectivamente. Inmediatamente presenta un multiformulario (wizard) que guía al usuario por los distintos pasos de la configuración básica. Finalmente, muestra la página de información de estado del cortafuegos con un conjunto de paneles donde se muestran varios gráficos con información relevante del funcionamiento del cortafuegos.

El siguiente paso será configurar la puerta de enlace por defecto. La interfaz de red WAN está configurada con su dirección IP, pero necesita una puerta de enlace que le permita enrutar los paquetes hacia la red WAN, valga la aclaración, en este caso Internet. La red del ICM se comunica con Internet mediante el enrutador CISCO por la dirección IP 200.55.136.169. Esta configuración se realiza por medio de la entrada de menú **System→Gateways**, donde se añade una nueva puerta de enlace, marcándola como puerta de enlace por defecto (Fig. 2.4).

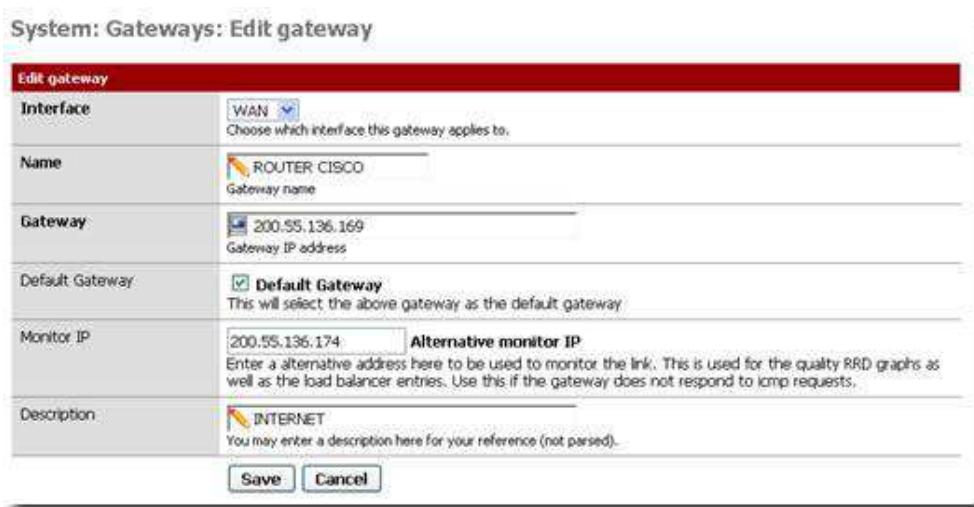


Fig. 2.4 Configuración de puertas de enlace de redes.

Ahora que el cortafuegos ya está listo para enrutar correctamente, se deben precisar algunos detalles específicos en la configuración del sistema. A esta sección se puede acceder desde el menú **System→General Setup** (Fig. 2.5).

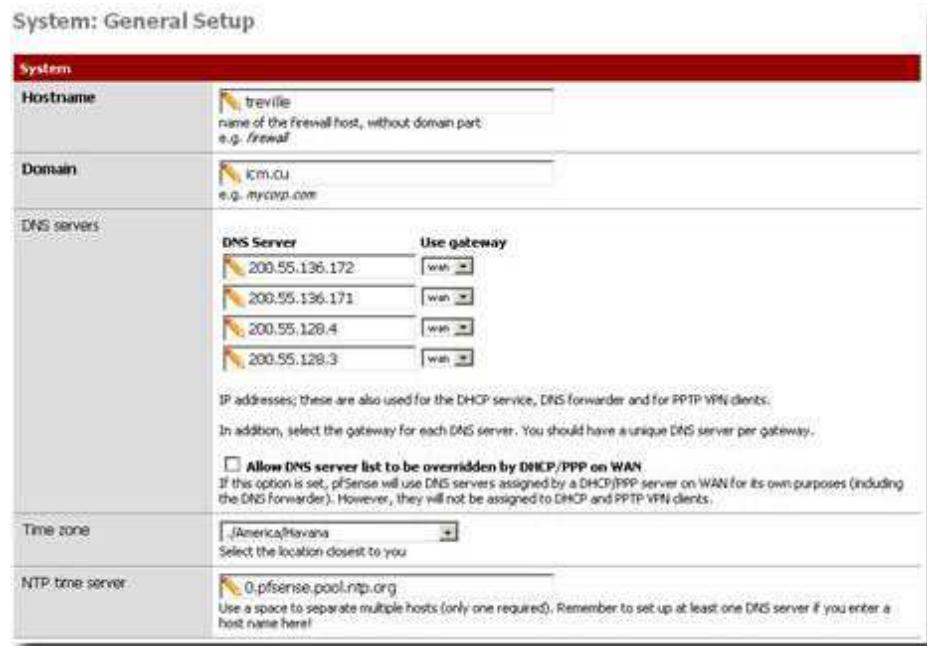


Fig. 2.5 Complemento de configuración de red del sistema.

## Aseguramiento.

La configuración primaria del cortafuegos pfSense brinda ya un nivel elevado de seguridad dado el propósito de mismo. Pero hay un grupo de tareas, en algunos casos necesarias, que se pueden realizar con vistas a asegurar el sistema y ajustarlo a diferentes necesidades.

Entre las tareas que no deben ser obviadas a la hora de garantizar una seguridad óptima del sistema están:

- Cambiar la contraseña del usuario **admin** de la Web. La contraseña por defecto es **pfsense**. En las últimas versiones esto se hace al final del wizard (guía por pasos) de configuración. Se dispone además de un usuario de acceso a la consola por SSH que es siempre **admin**. El cambio del nombre del usuario administrador vía web no afecta el del administrador vía SSH. Por el contrario, el cambio de contraseña sí afecta los dos modos de administración (SSH y Web). Este paso toma carácter obligatorio, pues de olvidarlo o saltarlo intencionalmente, permanece la contraseña por defecto del usuario **admin**, incurriendo en un problema de seguridad debido a que esta contraseña es pública.
- Cambiar la contraseña del usuario root del sistema. pfSense permite, al igual que FreeBSD el acceso a la administración del sistema mediante el shell de comandos. Por defecto el usuario root tiene la misma contraseña que el usuario **admin** de la web. Dejar cambiar esta contraseña también debilita la seguridad del sistema, incluso a aquellos a los que no se permite el acceso por shell, pues eventualmente un atacante que penetre utilizando algún agujero de seguridad de algún otro proceso, si conoce esta contraseña pudiera obtener el control absoluto del sistema haciendo uso de los privilegios de root.
- Habilitar la protección mediante el uso de contraseña del menú principal de la consola de administración. Si esta opción no es habilitada pfSense continuará mostrando este menú de consola, aún cuando se reinicia el sistema de modo que cualquier persona que tenga acceso físico al la PC que ejecuta pfSense tendrá acceso al menú. Con este menú se pueden realizar algunas tareas predefinidas de configuración y otras de administración como el acceso al shell de comandos con privilegios de administración. El mismo está diseñado pensando fundamentalmente en los usuarios que no están familiarizados con el shell de comandos.

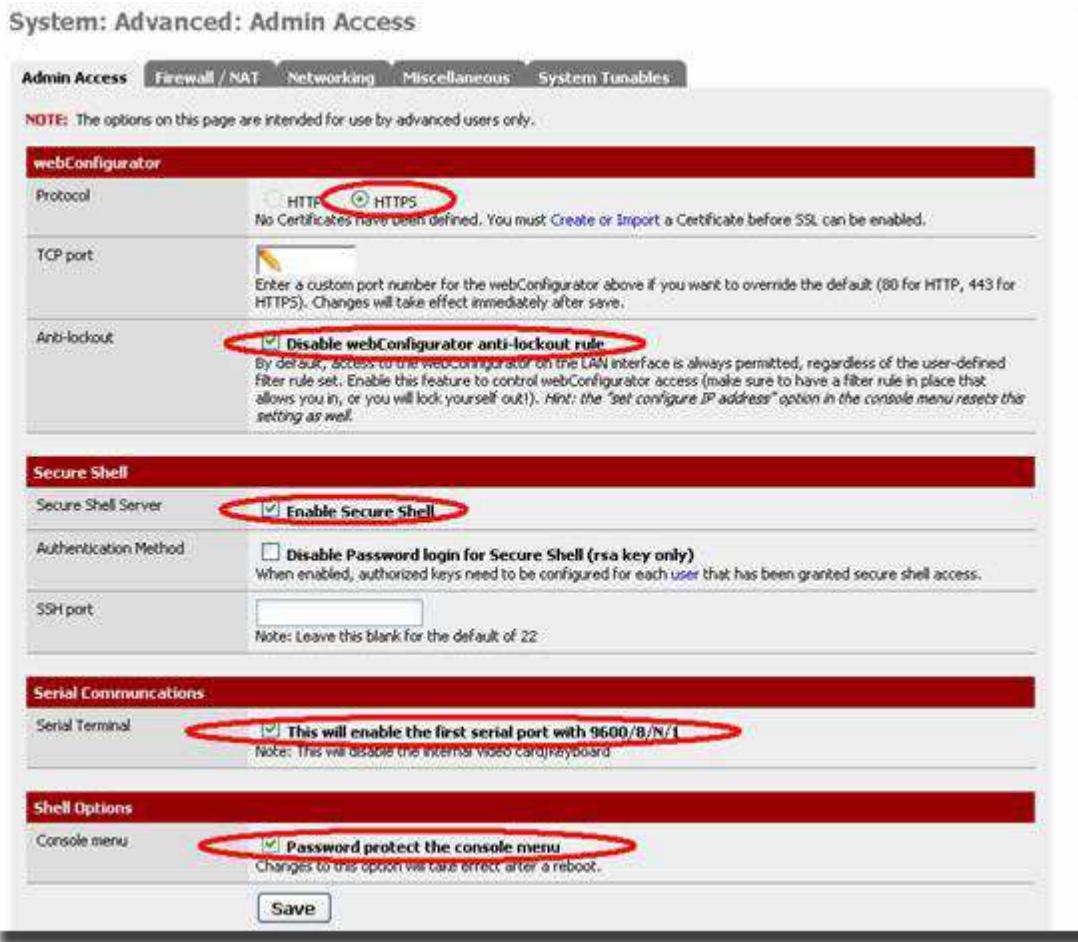


Fig. 2.6 Sección de seguridad del sistema en el panel de configuración.

Se cuenta con otras opciones que permiten ajustar la seguridad en un servidor pfSense (**Fig. 2.6**). En el menú **System → Advanced** se puede definir los tipos de acceso a la configuración. pfSense permite tres tipos de acceso al sistema:

1. Acceso vía web, es importante tener claro desde donde estará accesible el panel de configuración web y nivel de confianza que tenemos en la red o redes que tendrán acceso a la misma, pues de no tener plena confianza en los usuarios de la red, pfSense permite el uso el protocolo HTTPS para este propósito. El simple hecho de trabajar con la web puede traer implicaciones en la seguridad por lo que, teniendo en cuenta que configurar pfSense vía Web es muy cómodo, dicho acceso debe quedar asegurado.
2. Acceso al shell local o vía SSH. Bien desde el propio servidor accediendo desde el menú o desde otra máquina en la red mediante el protocolo SSH, pfSense permite el acceso al shell de comandos. Estos accesos se realizan implícitamente de forma bastante segura, pero es digno recordar que la máquina pfSense generalmente es el host bastión y lo que ello implica en cuestiones de seguridad. Se sugiere que este tipo de acceso se tenga bien controlado mediante certificados de seguridad, incluso es posible protegerlo mediante otros mecanismos de seguridad propios de los sistemas UNIX-like como son los TCP-wrappers.

3. Acceso a la consola vía puerto serie. Similar a los otros dispositivos, pfSense brinda el acceso desde el puerto serie del servidor. En entornos hostiles de seguridad es esta la única vía de acceso al cortafuegos que se recomienda por los especialistas más cautelosos.

### 2.2.3.2. Aislamiento físico y lógico de las subredes.

Otro aspecto relevante es el de la organización lógica de la red. La red debe estar organizada tanto física como lógicamente, se debe precisar que función desempeña cada componente de la red y que lugar ocupará en la misma (Ej. no se debe poner un servidor en la oficina de personal o de atención a cliente, como tampoco debemos poner las impresoras compartidas en el área destinada a los servidores, etc.). Tanto los componentes, como las áreas de la red deben tener restricciones de acceso apropiadas.

En la organización, fundamentalmente la lógica, una cuestión preponderante debe ser el esquema de direccionamiento de la red. En el esquema de direccionamiento de las distintas subredes intervienen la distribución de las direcciones IP y la resolución de direcciones mediante nombres de dominio que es realizada por los servidores de nombres de dominio.

#### Direccionamiento IP

Las direcciones IP son números binarios de 32 bits, o conjunto de números, que identifica únicamente a una estación de trabajo en una red de tipo IP. Las direcciones IP operan en la capa de red de modelo de protocolos de redes TCP/IP y es independiente de la dirección MAC en la capa inferior de enlace, como es el caso de la dirección MAC de las redes Ethernet. Teóricamente en Internet puede haber alrededor de 4 billones de direcciones de hosts. Esto nos hace pensar que hay más que suficiente pero TCP/IP impone algunas restricciones en el modo de asignar direcciones. Estas restricciones limitan severamente el número de direcciones realmente usables, donde un tanto más de la mitad han sido ya asignadas. Sin embargo, nuevos esquemas para trabajar con direcciones IP han sido implementados, en un nuevo estándar de direcciones de 128 bits (conocido como IPv6 en alegoría a la versión 6 del conjunto de protocolos TCP/IP) que va ganando aceptación progresivamente, sobre todo por el soporte de retro-compatibilidad.

Entre los esquemas de direccionamiento IP existen algunos más complejos, como la asignación de direcciones de redes mediante subnetting<sup>3</sup>, y otros más sencillos como el esquema de direcciones de red independientes donde las distintas redes se comunican entre sí a través de los enruteadores. Es esencial que el esquema de direccionamiento de la red cumpla cierto patrón lógico, sobre todo en las redes más complejas, o sea redes que estructuralmente están formadas por otras subredes bien sean físicas, refiriéndonos al cableado, o lógicas, refiriéndonos al esquema de direccionamiento.

<sup>3</sup> Subnetting, es una técnica mediante la cual se pueden usar más eficientemente los 32 bits de una dirección IP, creando redes que cuyas escalas no están limitadas por la Clases A,B o C de direcciones IP. Con esta técnica se pueden crear redes con límites en la cantidad de hosts mas ajustados a las necesidades reales.

Como se puede ver en la figura hemos optado por el modelo de redes independientes, o sea, todas las subredes internas tendrán direcciones de red privadas de clase C, o sea en el rango de las subredes 192.168.X.0/24, con máscara 255.255.255.0. Una de las ventajas de la utilización de direcciones IP privadas, es que la topología de la red queda escondida detrás del cortafuegos con lo que incrementa la seguridad de toda la red.

Según el análisis realizado, este modelo es suficiente pues la red interna cuenta con un aproximado de 80 estaciones de trabajo de modo que, incluyendo los dos servidores que en el futuro prestarán servicios en esta subred, no será necesario utilizar rango mayor de direcciones (clases A o B), pues duplicar o triplicar esta cifra es un proceso que puede tardar años.

El problema de este modelo, como planteábamos anteriormente, es que necesita un enrutador para comunicar las distintas subredes. Es aquí donde entra a jugar el cortafuegos, ya que por su naturaleza también desempeña la función de enrutador. Aunque esta es una razón de peso para la ubicación del cortafuegos, no es la única, pues sería fácilmente sustituible por un enrutador. Existen otras razones por la que el cortafuegos se encuentra en esta posición en la red. Una de las ventajas con respecto a los enrutadores convencionales es que puede mantener un mejor control sobre la información que se intercambia entre las diferentes subredes mediante diferentes mecanismos de filtrado. El resto de las razones las veremos en los epígrafes que siguen.

#### 2.2.3.2.1. Esquema de direccionamiento IP.

A continuación pasamos a describir el esquema de direccionamiento que se muestra en la figura (Fig. 2.7a):

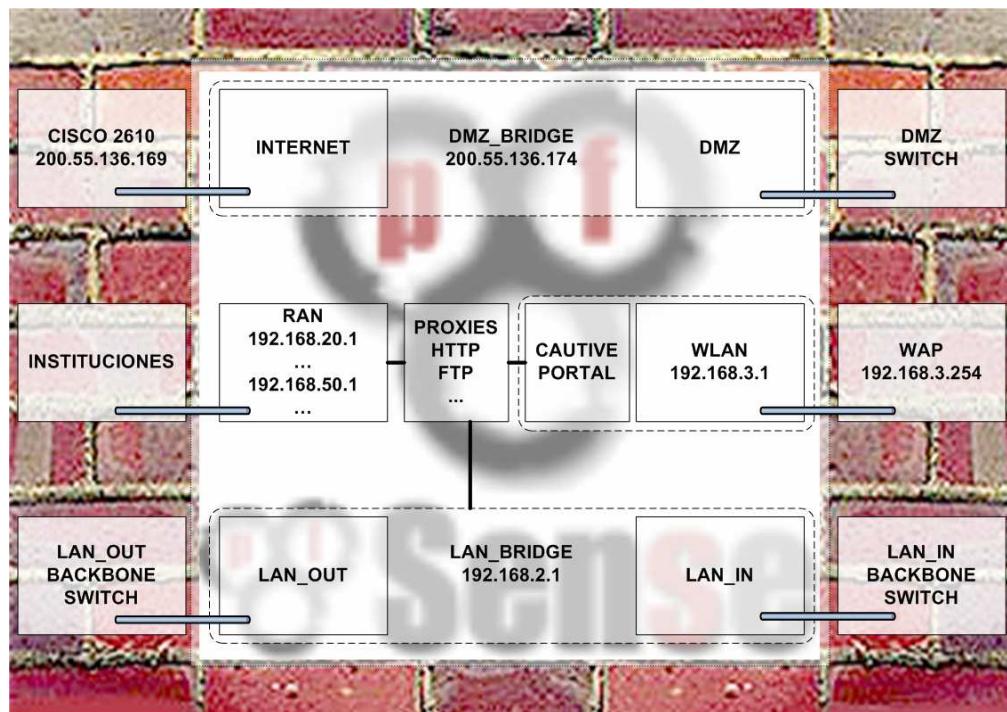


Fig. 2.7a Distribución de Interfaces de red en el cortafuegos.

El nuevo diseño de la red integra en la red del ICM varias subredes físicas y lógicas descritas en la siguiente tabla:

Nombre/NIC	Dirección de Red	Descripción
Internet (WAN)	200.55.136.168/29	La red ICM actualmente forma, aunque de reducida manera, parte de la Internet, cuenta con sólo 6 direcciones IP reales, descartando la dirección de red y la dirección de broadcast. Esta red está asignada por el ISP ENET dependencia de la empresa telefónica ETECSA.
Red interna (sección interior LAN_IN)	192.168.2.0/24	Red tipo LAN interna de la edificación principal del ICM. Esta LAN fue diseñada y montada por la empresa de proyectos Yuri Gagarin.
Red interna (sección exterior LAN_OUT)		Red tipo LAN del edificio aledaño, actualmente en reconstrucción, esta LAN será parte lógica de la del Instituto, pues desde esta red se deberá acceder a los recursos y servicios de la red local ya existente.
Inalámbrica (WLAN)	192.168.3.0/24	Red Inalámbrica de acceso a servicios de la red del ICM, enfocada principalmente al uso en laptops con soporte inalámbrico de las diferentes direcciones, equipos de uso temporal en puestos de mando y eventos similares, y otros dispositivos portátiles afines.
Instituciones (RAN)	192.168.10.0/24 192.168.20.0/24 ...	Red WAN conformada por las instituciones con acceso remoto a la red del Instituto, para utilizar el acceso a Internet, correo y otros servicios referentes a entidades de la música.

Tabla 2.1 Esquema de direcciones de redes propuesto.

Este proyecto está elaborado, basándose estrictamente con lo que dispone el Instituto actualmente, ya que, aunque se cuenta con la aprobación del presupuesto para la instalación de un nuevo enlace y la ampliación del ancho de banda, esto no implica que se amplíe el rango de direcciones IP reales, cuestión importante, teniendo en cuenta que se aspira a que nuestras dependencias tenga también presencia en Internet basada en direcciones reales, aunque existen otros mecanismos para lograr este objetivo..

También se muestra una propuesta anticipada para asignar direcciones a los componentes importantes dentro de las diferentes subredes, con esta idea se facilitaría el proceso de configuración del cortafuegos y los mecanismos de resolución de nombres de dominio, tanto para las redes internas como desde Internet:

Componente	Nombre(s) de dominio	Función		
		Red/NIC	Dirección IP	Breve Descripción
Enrutador	gateway.icm.cu	Internet	200.55.136.169	Enrutador CISCO Puerta de enlace de toda la red del ICM.
Cortafuegos	trevalle.icm.cu firewall.icm.cu	Internet (DMZ_BRIDGE)	200.55.136.174	Puente de red en el cortafuegos que comunica la sección externa de la WAN con la DMZ.
		Red interna (LAN_BRIDGE)	192.168.2.1	Puente de red en el cortafuegos que comunica las dos secciones de la red LAN.
		(Red de Instituciones) (RAN)	192.168.20.1 ... 192.168.50.1 ...	Subredes privadas de acceso remoto de instituciones de la música
		Inalámbrica (WIFI)	192.168.3.1	Puerta de enlace a los servicios internos para los dispositivos inalámbricos
Punto de Acceso Inalámbrico	-	Inalámbrica (WIFI)	192.168.3.254	Dirección IP que necesita el punto de acceso para integrarse en la red.
Servidor Web y DNS1	aramis.icm.cu www.icm.cu (dominios de web) ns1.icm.cu	Internet (DMZ)	200.55.136.171	Dirección mediante la cual se accederá desde Internet a los servicios de la Web y DNS.
Servidor de Correos y DNS2	dartagnan.icm.cu mail.icm.cu (MX) (dominios de correo) ns2.icm.cu	Internet (DMZ)	200.55.136.172	Dirección para el intercambio de todo el correo y DNS de respaldo.
Servidor Proxy (interno)	athos.icm.cu proxy.icm.cu intranet.icm.cu	Red interna	192.168.2.2	Servidor Proxy de la red interna para la navegación de los usuarios.
Servidor NAS	porthos.icm.cu salva.icm.cu	Red interna	192.168.2.3	Servidor de almacenamiento, salva y otros servicios internos.

Tabla 2.2 Configuración de red propuesta para los componentes principales de la red ICM.

## pfSense como enrutador

La configuración del cortafuegos consta de dos etapas lógicas, en la primera consiste en convertir el host bastión un enrutador que nos permite la comunicación entre las redes internas, y entre la DMZ y la Internet. Entre las redes internas y la DMZ no hay comunicación (ruta), pues cumple cabalmente con el concepto de DMZ. En una segunda etapa pasamos a establecer las políticas de seguridad y controles de acceso acordes con las directivas de seguridad de nuestra empresa. Esto se hará utilizando los mecanismos de seguridad que brinda pfSense.

Una de las ventajas que brinda la utilización del esquema de puentes (**Fig. 2.7b**) que se propone a continuación es el ahorro de direcciones IP, pues será posible notar que el cortafuegos, a pesar de tener 6 interfaces físicas (y otras tanta virtuales o lógicas, si se utiliza VLAN), una pareja de interfaces conecta cada red (externa con DMZ y segmentos de la red interna), solo consume una dirección IP en cada una de las redes que esta conectado tanto física como lógicamente. Esto puede no significar mucho en redes internas con esquemas de direcciones privadas, pero para el caso de la DMZ es una solución muy interesante pues utilizando dos interfaces comunica la DMZ y la Internet utilizando solo una (o ninguna) de las escasas direcciones públicas.

Interface	Network port
DMZ	r0 (00:40:54:0b:81:9e)
LAN_IN	r1 (00:40:f4:27:fd:a6)
LAN_OUT	r2 (00:e0:7d:7c:71:e5)
DMZ_BRIDGE	BRIDGE0 (DMZ_BRIDGE)
LAN_BRIDGE	BRIDGE1 (LAN_BRIDGE)
WAN	fxp0 (00:01:00:2a:c0:81)

Fig. 2.7b Distribución de interfaces y puentes de red en el cortafuego.

La figura que sigue muestra el panel principal de los cortafuegos sirviendo de enrutador (con los filtros desactivados) a las redes configuradas anteriormente:

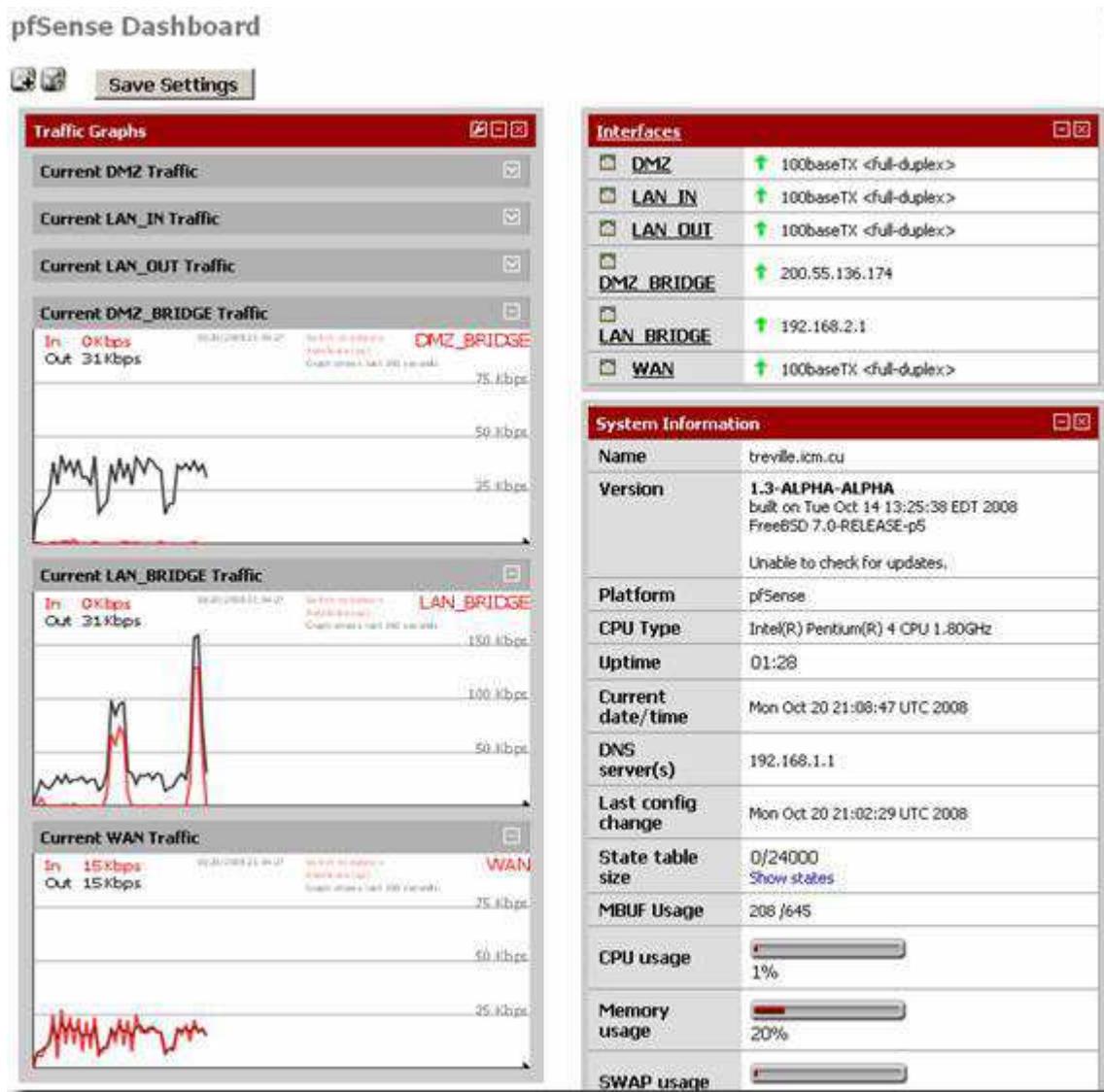


Fig. 2.8 Página principal del panel de configuración web de pfSense.

### 2.2.3.3. Creación de la subred DMZ.

En cuestiones de seguridad informática, una **zona desmilitarizada**<sup>4</sup> (DMZ) o **red perimetral** es una red local (una subred) que se ubica entre la red interna de una organización y una red externa, generalmente Internet. El objetivo de una DMZ es que las conexiones **a** la DMZ desde la red interna y la externa estén permitidas, mientras que las conexiones **desde** la DMZ **sólo** se permitan a la red externa -- los equipos (hosts) en la DMZ **no** pueden conectar con la red interna. Esto permite que los equipos (hosts) de la DMZ puedan dar servicios a la red externa a la vez que se protege la red interna en el caso de que intrusos comprometan la seguridad de los equipos (hosts) situados en la zona desmilitarizada. Para cualquiera que desde la red externa que quiera conectarse ilegalmente a la red interna, la zona desmilitarizada se convierte en un callejón sin salida, cortando la visibilidad hacia la red o redes internas.

La DMZ se usa habitualmente para ubicar servidores que es necesario que sean accedidos desde fuera, como servidores de Correo, Web y DNS. Al contrario de lo que sugiere el término, las DMZ son zonas semiprotegidas, o sea que la protección de los equipos en la DMZ es limitada dado que los servicios que prestan estos suelen ser públicos hacia la Internet, esto implica riesgos de seguridad y suelen ser propensos a ataques, por lo que se debe tener mucho cuidado con las interacciones entre la DMZ y las redes internas, sobre todo en los accesos a las redes internas.

La ausencia de una DMZ, suele provocar la adopción de políticas débiles de seguridad por parte de los grupos informáticos, principalmente cuando se le confían los servicios públicos a máquinas que se encuentran en las redes internas. Existen muchos ejemplos, de los daños que puede provocar la aplicación de políticas de seguridad relajadas para casos de conveniencia.

#### 2.2.3.3.1. Topología de la DMZ.

Uno de los procesos dentro de la instalación de un cortafuegos en una empresa dada que requiere ser cuidadosamente considerado y planeado es la creación de la DMZ, pues del mismo modo que esto hace más compleja la topología de la red, tiene importantes beneficios en el incremento de la seguridad de la red y los servicios que se prestan hacia las distintas redes internas e Internet.

Existe diversidad de modelos en la creación de una DMZ [11a][11b], entre ellos uno del más extendido es el modelo de trípode (three-Legged) con un cortafuegos de múltiples interfaces (Multi-Homed). Este modelo suele combinarse con otros modelos como el de enrutador-bastión (screened-host o choke-gate), es decir, el enrutador es la primera y más importante línea de defensa.

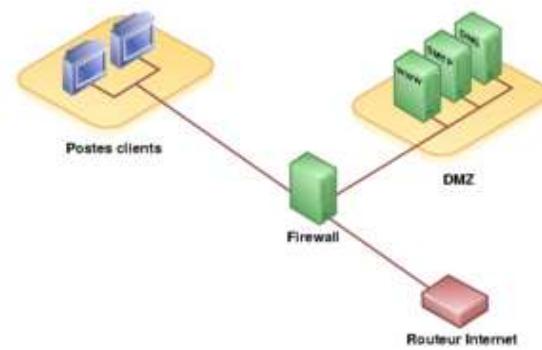


Fig. 2.9 Diagrama de DMZ con cortafuegos de trípode.

<sup>4</sup> El término **zona desmilitarizada** es tomado de la franja de terreno neutral que separa a ambas Coreas, y que es una reminiscencia de la Guerra de Corea, aún vigente y en tregua desde 1953. Paradójicamente, a pesar de que esta zona desmilitarizada es terreno neutral, es una de las más peligrosas del planeta, y por ello da nombre al sistema **DMZ**.

Mientras que el enrutador (choke) se encarga de filtrar los paquetes que se puedan considerar peligrosos para la seguridad de la red interna, permitiendo únicamente la comunicación con un reducido número de servicios, en la máquina bastión, dotada con características de cortafuegos y único sistema accesible desde el exterior, se realizan tareas de defensa más sofisticadas que suelen estar relacionadas con el análisis del contenido de los paquetes, además en muchas ocasiones se ejecutan proxies de aplicación a los que acceden fundamentalmente las máquinas en la red interna, pues los hosts de la DMZ por lo general son servidores de producción con servicios públicos [A].

En la mayoría de los casos es más fácil de proteger un enrutador que una máquina con un sistema operativo de propósito general, como los BSDs, que además por definición ha de ofrecer ciertos servicios: no tenemos más que fijarnos en el número de problemas de seguridad que afectan a por ejemplo a IOS (el sistema operativo de los enrutadores Cisco), muy reducido frente a los que afectan a diferentes sistemas UNIX-like.

Por estos matices se conciente en que esta configuración ofrece robustez en la seguridad, es bien aceptada por una parte mayoritaria de los expertos en seguridad informática, sobre todo para redes pequeñas y medianas, pues si bien es cierto que existen diseños más complejos, por lo general van acompañados de grandes inversiones en equipamientos de seguridad, razón por la cual suelen ser más sugerentes para redes de grandes dimensiones o redes de seguridad máxima.

Entonces llegamos a que, cuando una máquina de la red interna desea comunicarse con el exterior existen dos posibilidades:

1. El choke permite la salida de algunos servicios a todas o a parte de las máquinas internas a través, pasando o no por el cortafuegos, de un simple filtrado de paquetes.
2. El choke prohíbe todo el tráfico entre máquinas de la red interna y el exterior, permitiendo sólo la salida de ciertos servicios que provienen de la máquina bastión y que han sido autorizados por la política de seguridad de la organización. Así, estamos obligando a los usuarios a que las conexiones con el exterior se realicen a través de los servidores proxy situados en el bastión.

Finamente es necesario aclarar que un bastión que enlaza varias (5) subredes aparentemente no se enmarca dentro del modelo de trípode. En efecto el diseño propuesto es una extensión del modelo en cuestión, pues solo una de las subredes adquiere la categoría de DMZ.

La DMZ se distingue fácilmente por dos elementos fundamentales, sus direcciones IP están en el rango de direcciones públicas de la Institución y estará conformada solo por los servidores de producción que deberán brindar servicios igualmente públicos. El resto de las subredes serán redes internas, con rangos de direcciones IP privadas y brindaran servicios solo a la propia subred y en algunos casos a otras subredes dentro de su misma categoría, nunca al exterior.

Esta alternativa permite aprovechar las características de enrutador implícitas en el cortafuegos, pues de lo contrario fuese necesario invertir recursos para la adquisición de un enrutador profesional dedicado. Añadiendo que se obtienen beneficios en la seguridad ya que el enrutado se combina con los filtros del cortafuegos, de esta manera se incrementa también la protección interior-interior (término que se comentaba a inicios del capítulo) entre las distintas subredes.

### 2.2.3.3.2. Configuración de la DMZ en pfSense.

Explicado conceptualmente el modelo físico de la nueva topología de la red se procede a mostrar como se configura pfSense para dar soporte la arquitectura propuesta. Tomaremos como punto de partida la configuración inicial de pfSense propuesta en los subepígrafes anteriores, teniendo en cuenta también el esquema de direccionamiento.

Según el modelo de trípode, el cortafuegos deberá tener como mínimo tres interfaces, en algunos sistemas es posible enlazar varias subredes a una misma interfaz mediante la configuración de varias direcciones IP, pero por muchas razones, entre ellas con mayor peso las de seguridad esto no es lo deseado, por lo que esto solo se debe hacer en un caso de extrema necesidad o conveniencia, lo que no se ajusta a nuestro caso. pfSense cataloga como interfaces opcionales de la tercera en adelante, o sea, la primera será la WAN la segunda la LAN y el resto OPT1, OPT2, y así sucesivamente.

Nota: Antes de comenzar a configurar las interfaces es recomendable deshabilitar la función de cortafuegos, de esta manera pfSense actúa solo como enrutador. Esto nos facilita en gran medida el trabajo de la configuración de las rutas, pues las reglas de los filtros pueden obstruir rutas válidas. Para deshabilitar esta funcionalidad debemos ir a **System ➔ Advanced ➔ Firewall/NAT** donde marcaremos la opción **Disable firewall filtering**. También es importante luego configurar apropiadamente el cortafuegos y activarlo nuevamente para que desempeñe su función.

Configurar la DMZ es establecer una ruta para los paquetes en ambos sentidos, desde la Internet hacia la DMZ y en sentido opuesto. Siguiendo las indicaciones de la tabla de direccionamiento que se presenta en el epígrafe del esquema de direccionamiento IP, la interfaz de la DMZ toma la dirección 200.55.136.174/29. Asignar una dirección IP pública a la interfaz de la DMZ no bastará para comunicar la subred DMZ con Internet, no existe una ruta entre la WAN y la DMZ.

Quizás alguna lógica sugiere convertir la interfaz WAN en la puerta de enlace de la interfaz DMZ, esto solo garantiza una ruta, el flujo que va de la DMZ a la WAN y no en sentido opuesto. No se puede entonces configurarle a la WAN, la DMZ como puerta de enlace, pues quedaría restringida la salida a la Internet, además provocaría un ciclo infinito entre la WAN y la DMZ en el flujo de información. Otro de los problemas es que en la tabla de rutas no es posible crear una ruta especial solo para las IPs de la DMZ, de hecho solo es posible crear rutas a redes externas, como indica una nota aclaratoria, en el panel de configuración de rutas, haciendo esta salvedad.

Este problema se resuelve mediante los puentes de red (bridge) por software [E]. Se denominan así por que emulan el funcionamiento de los puentes de hardware que en ocasiones se utilizan para incrementar las distancias de los tramos de red o para conectar dos o más redes. La función de puente por hardware también puede verse en los commutadores de red que comunican a las distintas máquinas de la red.

También como se podrá ver más adelante que con pfSense es posible utilizar estos puentes como puentes de filtrado, al activar los mecanismos de seguridad, en las diferentes interfaces, incrementando los niveles de seguridad en las diferentes subredes.

Ahora podemos dar paso a configurar el puente que conectará la DMZ con la WAN:

1. Primeramente se configura la interfaz WAN (**Interfaces** ➔ **WAN**), dejándola sin dirección IP y especificando **Type** como **None** (**Fig. 2.10**).



Fig. 2.10 Configuración de la interfaz WAN.

2. Se crea el puente entre las interfaces WAN y DMZ. (**Interfaces** ➔ **Assign** ➔ **Bridges**). Esto genera una nueva interfaz, la interfaz virtual del puente bridge0, la que es posible visualizar y añadir al menú de interfaces (**Interfaces** ➔ **Assign** ➔ **Interface Assignments**).
3. Se configura el puente, sustituto ahora de la interfaz WAN, será nombrado DMZ\_BRIDGE (**Interfaces** ➔ **DMZ\_BRIDGE**) y tomará la dirección IP estática 200.55.136.174/29 (**Fig. 2.11**).

**Interfaces: DMZ\_BRIDGE**

**General configuration**

**Enable Interface**

Description	<input type="text"/> DMZ_BRIDGE Enter a description (name) for the interface here.
Type	Static <input type="button"/>
MAC address	<input type="text"/> <input type="button"/> Copy my MAC address This field can be used to modify ("spoof") the MAC address of the WAN interface. (may be required with some cable connections) Enter a MAC address in the following format: xxx:xxxx:xxxx or leave blank.
MTU	<input type="text"/> <input type="button"/> If you enter a value in this field, then MSS clamping for TCP connections to the value entered above minus 40 (TCP/IP header size) will be in effect. If you leave this field blank, an MTU of 1492 bytes for PPPoE and 1500 bytes for all other connection types will be assumed.

**Static IP configuration**

IP address	<input type="text"/> 200.55.136.174 /29 <input type="button"/>
Gateway	CISCO <input type="button"/> Select a existing Gateway from the list or add one on the Gateways page

Save

Fig. 2.11 Configuración de la interfaz virtual DMZ\_BRIDGE.

- Finalmente se pasa a configurar la interfaz DMZ(**Interfaces**➔**DMZ**). Antes de proceder con la configuración será necesario cambiar el nombre de la interfaz LAN (**Interfaces**➔**LAN**), en alegoría a la nueva función, ahora por DMZ. El procedimiento es el mismo que se realizó con la WAN (**Fig. 2.12**).

**Interfaces: DMZ**

**General configuration**

Description	<input type="text"/> DMZ Enter a description (name) for the interface here.
Type	None <input type="button"/>
MAC address	<input type="text"/> <input type="button"/> Copy my MAC address This field can be used to modify ("spoof") the MAC address of the WAN interface. (may be required with some cable connections) Enter a MAC address in the following format: xxx:xxxx:xxxx or leave blank.
MTU	<input type="text"/> <input type="button"/> If you enter a value in this field, then MSS clamping for TCP connections to the value entered above minus 40 (TCP/IP header size) will be in effect. If you leave this field blank, an MTU of 1492 bytes for PPPoE and 1500 bytes for all other connection types will be assumed.

Save

Fig. 2.12 Configuración de la interfaz DMZ.

Nota: El paso de la configuración de la interfaz DMZ se ha dejado, intencionalmente, para el final ya que al aplicar los cambios, se pierde la comunicación al instante con la interfaz DMZ (anteriormente interfaz LAN) y como consecuencia se pierde también el acceso al panel de configuración web. Para continuar con la configuración del cortafuegos será necesario acceder desde otra interfaz de red, por ejemplo en el caso que ocupa puede hacerse ahora en la URL <http://200.55.136.174>, o sea desde una máquina en la DMZ.

De esta manera queda listo ya el puente de la DMZ. Se puede comprobar la disponibilidad de las rutas mediante el comando ping, o sea el envío de paquetes ICMP de comprobación, entre la sección exterior, intermedia, e interior.

#### 2.2.3.4. Configuración de la subred LAN.

Como se ha mencionado la red local del instituto quedará dividido en dos secciones, la sección interna representa la red ya existente y la sección externa representa nueva red que se instalará en la edificación en construcción actualmente.

En el procedimiento para la configuración de redes internas lo primero que será necesario tener en cuenta es que las dos secciones de la red forman parte de la misma red lógica, o sea que, de no ser necesario, no deben quedar separadas ni en el esquema de direcciones y el por el cableado físico, pues deben compartir los mismos recursos y servicios.

Una solución simplista sería conectar la red externa directo al commutador (switch) backbone, pero es posible también utilizar las capacidades del cortafuegos, y de esta manera aprovechar la ventaja que nos brinda al mantener una comunicación controlada entre las dos subredes, que luego puede ser de utilidad para cuestiones de monitoreo, estadísticas y seguridad en general, dejando la variante simple para casos de catástrofes.

Para realizar esta tarea se utiliza el mismo procedimiento de puente que se utilizó entre la WAN y DMZ, esta vez las interfaces será OPT1 renombrada a LAN\_IN y la OPT2 renombrada a LAN\_OUT. A continuación se muestra de forma sintetizada y gráfica, aprovechando que se ha mencionado anteriormente, el procedimiento completo:

1. Configuración de la interfaz LAN\_IN

**Interfaces: LAN\_IN**

**General configuration**

**Enable Interface**

Description	LAN_IN Enter a description (name) for the interface here.
Type	None
MAC address	<input type="text"/> Copy my MAC address This field can be used to modify ("spoof") the MAC address of the WAN interface (may be required with some cable connections) Enter a MAC address in the following format: xxx:xxxx:xxxx or leave blank
MTU	<input type="text"/> If you enter a value in this field, then MSS clamping for TCP connections to the value entered above minus 40 (TCP/IP header size) will be in effect. If you leave this field blank, an MTU of 1492 bytes for PPPoE and 1500 bytes for all other connection types will be assumed.

**Save**

Fig. 2.13 Configuración de la interfaz LAN\_IN.

2. Configuración de la interfaz LAN\_OUT (En este caso no es necesario hacerlo al final).

**Interfaces: LAN\_OUT**

**General configuration**

**Enable Interface**

Description	LAN_OUT Enter a description (name) for the interface here.
Type	None
MAC address	<input type="text"/> Copy my MAC address This field can be used to modify ("spoof") the MAC address of the WAN interface (may be required with some cable connections) Enter a MAC address in the following format: xxx:xxxx:xxxx or leave blank
MTU	<input type="text"/> If you enter a value in this field, then MSS clamping for TCP connections to the value entered above minus 40 (TCP/IP header size) will be in effect. If you leave this field blank, an MTU of 1492 bytes for PPPoE and 1500 bytes for all other connection types will be assumed.

**Save**

Fig. 2.14 Configuración de la interfaz LAN\_OUT.

### 3. Creación del puente entre las dos interfaces



Fig. 2.15 Configuración de puentes de red en pfSense.

### 4. Configuración del puente

**General configuration**

**Enable Interface**

**Description**: LAN\_BRIDGE  
Enter a description (name) for the interface here.

**Type**: Static

**MAC address**:  Copy my MAC address  
This field can be used to modify ("spoof") the MAC address of the WAN interface (may be required with some cable connections)  
Enter a MAC address in the following format: xxx:xxx:xxx:xxx or leave blank

**MTU**:   
If you enter a value in this field, then MSS clamping for TCP connections to the value entered above minus 40 (TCP/IP header size) will be in effect. If you leave this field blank, an MTU of 1492 bytes for PPPoE and 1500 bytes for all other connection types will be assumed.

**Static IP configuration**

**IP address**: 192.168.2.1 / 24

**Gateway**: None Select a existing Gateway from the list or add one on the Gateways page

**Save**

Fig. 2.16 Configuración de la interfaz virtual LAN\_BRIDGE.

#### 2.2.3.4.1. DHCP y DNS.

Para la asignación automática de direcciones se puede utilizar el servidor DHCP que ofrece el pfSense, o simplemente disponer otro servidor para esta tarea conectado en la red local. pfSense pone a la disposición de sus usuarios un agente de relevo DHCP, que en los casos de los puentes de red solo será necesario habilitarlo si los filtros no permiten el paso de este protocolo.

Por otro lado, para la resolución de nombres pfSense dispone similares mecanismos a los del servicio de DHCP. Un DNS de reenvío (forwarder) que puede ser utilizado para resolver tanto las direcciones internas como las externas, sirviendo de relevo a diferentes servidores. Además en la paquetería de pfSense trae un servidor de nombre ligero que se puede integrar en la interfaz web de administración.

### 2.2.3.5. Configuración de la subred WLAN.

Los ordenadores y dispositivos informáticos en red ofrecen un gran potencial en la gestión del trabajo de cualquier empresa, pero las redes tradicionales implican la conexión física de cables a cada ordenador, en cada oficina y en cada edificio. Es una red cara y poco flexible que usualmente limita la incorporación de nuevos dispositivos, y que con un ligero aumento de la distancia imposibilita totalmente la conectividad.

En cambio, con las redes inalámbricas se puede conectar hasta locales enteros de una forma rápida y asequible, incluso en diferentes edificios, cualquier dispositivo con soporte que se encuentre en el radio del punto de acceso, podrá conectarse sin necesidad de habilitar nuevo cableado. Una red inalámbrica es portátil, flexible y de fácil ampliación. En comparación con la red cableada, el ahorro en costes de instalación y de configuración es significativo. No hay que descifrar complejos esquemas de cableado ni contratar personal calificado para la instalación.

Además, en cuanto a los cambios tecnológicos, las redes inalámbricas se integran fácilmente en las redes existentes y es capaz de funcionar y comunicar con los sistemas más antiguos. La incorporación de una red inalámbrica depende tan solo de la instalación de los puntos de acceso y la tecnología de conexión en aquellos dispositivos que no vengan ya con el soporte incorporado.

#### 2.2.3.5.1. Configuración del punto de acceso.

En el Instituto se cuenta actualmente con un dispositivo de punto de acceso inalámbrico *Netgear WG302v2* con un radio promedio de alcance de 30 m y un ancho de banda que fluctúa con la distancia en un rango cercano a los 54 Mb/s en compatibilidad con el modo IEEE 802.11g. En el **Anexo II.D** se pueden leer las especificaciones técnicas de este dispositivo.

Entre las herramientas que más utilidad brindan de este dispositivo están, la configuración mediante la interfaz web y el soporte de archivo de configuración (**Fig. 2.17**), de modo que permite hacer la salva de la configuración y en caso de catástrofe recuperarla nuevamente.

La instalación física de este dispositivo es sumamente sencilla pues solamente será necesario conectarlo a la corriente y a uno de los puertos que bien puede ser en un commutador o directamente al cortafuegos.

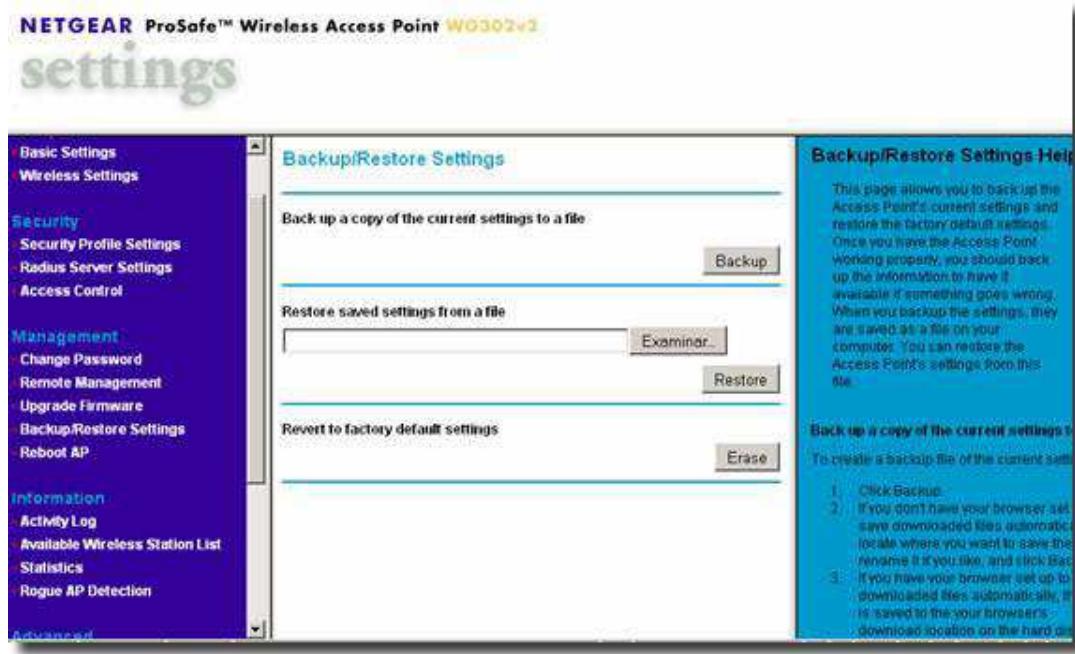


Fig. 2.17 Panel de configuración web del punto de acceso inalámbrico.

Para la conectividad lógica, o sea, la transmisión de datos, puede configurarse igualmente de dos maneras. Cuando está conectado directamente al cortafuegos, caso en que se cuenta con una interfaz de red exclusivamente para dar conectividad a la red WLAN. En otro caso es posible utilizar el modelo de VLAN, que fue explicado al inicio del capítulo, pues tanto el punto de acceso como el cortafuegos pfSense brindan soporte para este tipo de configuración de red, solo restaría la disponibilidad de un commutador (switch) con soporte para VLAN. Ahora asumiendo que se cuenta ya con el material requerido se prosigue con la configuración.

Primeramente será necesario seleccionar la interfaz de red que utilizaremos en el cortafuego (**Fig. 2.18**). Creamos una subred VLAN (**Interfaces** → **Assign** → **VLANs**) en dicha interfaz:

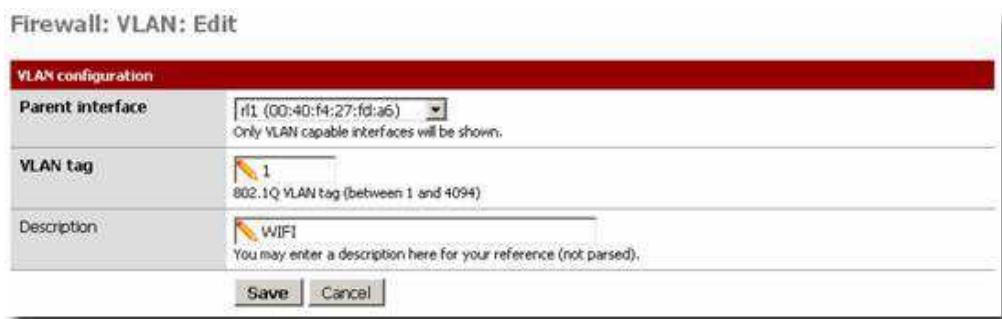


Fig. 2.18 Creación de la interfaz (VLAN) virtual para la subred inalámbrica.

Es importante notar que esta interfaz comparte las conexiones de varias redes disjuntas, por lo que el resto de las subredes configuradas en la misma interfaz deben usar igualmente el modelo de VLAN (luego incluir en las distintas VLANs el puerto en el conmutador). El identificador de la VLAN (tag) será en número 1, pues es el que trae por defecto configurado el punto de acceso.

A continuación se incluye la nueva interfaz para la VLAN en la lista de las interfaces del cortafuegos (**Interfaces**→**Assign**→**Interface Assignments**), para entonces configurarla (**Interfaces**→**WLAN**) (Fig. 2.19):



Fig. 2.19 Configuración de la interfaz WLAN.

Como se había explicado anteriormente se utiliza la subred privada 192.168.3.0/24. Siendo el cortafuegos la 192.168.3.1 y el punto de acceso la 192.168.3.254. De este modo si se configura el punto de acceso con esta dirección (Fig. 2.20) se establece la comunicación entre ambos extremos.

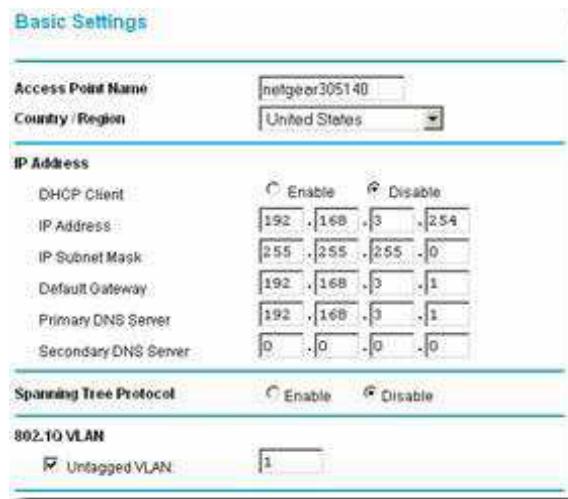


Fig. 2.20 Configuración de red del punto de acceso.

Una vez verificada la comunicación entre el punto de acceso (comando ping) y el cortafuegos se puede configurar la conectividad de los clientes. Es muy común en redes inalámbricas la asignación de la configuración de red mediante DHCP. El punto de acceso tiene incorporado este servicio, pero por cuestiones técnicas, se utiliza esta prestación desde el propio cortafuegos pfSense.

Para utilizar el servicio DHCP desde pfSense se configura el servidor DHCP atendiendo solicitudes en la interfaz 192.168.3.1 (**Fig. 2.21**). La configuración de red del punto de acceso estará igualmente controlada por el servidor DHCP, mediante la reservación de direcciones IP por MAC, el resto de los cliente obtienen una dirección disponible en el rango 192.168.3.20 – 192.168.3.40, que permite 20 dispositivos conectados, este rango puede ser incrementado en correspondencia con las necesidades.

The screenshot shows the 'Services: DHCP server' configuration page. The 'WLAN' tab is selected. Key settings include:

- Enable DHCP server on WLAN interface**: Checked.
- Deny unknown clients**: Unchecked.
- Subnet**: 192.168.3.0
- Subnet mask**: 255.255.255.0
- Available range**: 192.168.3.0 - 192.168.3.255
- Range**: 192.168.3.20 to 192.168.3.40
- WINS servers**: Two entries, both deleted.
- DNS servers**: One entry: 192.168.3.1. A note states: "NOTE: leave blank to use the system default DNS servers - this interface's IP if DNS forwarder is enabled, otherwise the servers configured on the General page."
- Gateway**: 192.168.3.1. A note states: "The default is to use the IP on this interface of the firewall as the gateway. Specify an alternate gateway here if this is not the correct gateway for your network."
- Domain-Name**: A dropdown menu with options: "use the domain name from the interface", "specify an alternate domain name", and "specify an alternate domain suffix".

At the bottom, there is a table for reserved IP addresses by MAC address:

MAC address	IP address	Hostname	Description
00:1b:2f:30:51:40	192.168.3.254	ICM-AP	WiFi Access Point

Fig. 2.21 Configuración del servidor DHCP en pfSense para la interfaz WLAN.

En las figuras (Fig.2.22) (Fig.2.23) se muestran los resultados de la asignación de direcciones por el servidor DHCP de pfSense y la conexión en el cliente:

Status: DHCP leases							
IP address	MAC address	Hostname	Start	End	Online	Lease Type	
192.168.3.20	00:0f:b5:ba:c7:59	informatica3	2008/10/25 09:21:33	2008/10/25 11:21:33	online	active	
192.168.3.254	00:1b:2f:30:51:40	ICM-AP	2008/10/25 09:36:53	2008/10/25 09:41:53	online	static	

Show all configured leases

Fig. 2.22 Resultados de lease DHCP en el servidor pfSense.

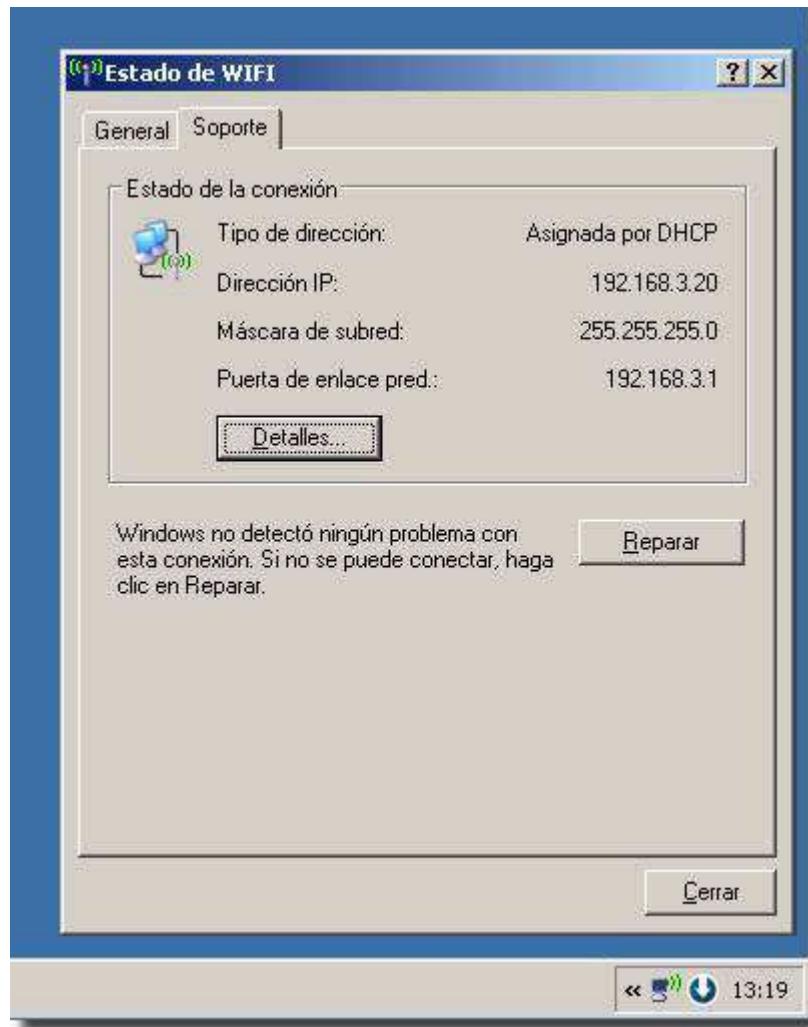


Fig. 2.23 Configuración del cliente haciendo uso del servidor DHCP.

En este punto se tiene la red inalámbrica funcionando, lista para que se conecten los clientes, solo resta definir las políticas de seguridad y control de acceso para esta subred, pues se ha utilizado para la conexión el modelo de libre acceso (open access), o sea, el SSID [12] es público y cualquiera con un dispositivo de red inalámbrica puede conectarse a la misma. Esto generalmente no trae implicaciones mayores si se controlan correctamente los accesos que los clientes conectados pueden tener, ejemplo de ellos son los accesos a redes internas y/o a la Internet. En caso de presentarse alguna incidencia que viole los controles de acceso en esta subred se puede acudir a opciones de seguridad más avanzadas que son soportadas por la configuración del punto de acceso.

#### 2.2.3.5.2. Portal Cautivo.

Según se plantea en el epígrafe anterior se ha depositado la seguridad de la red inalámbrica en el control de los accesos de los clientes conectados. Esto significa que se utiliza algún mecanismo que combinado con las reglas de filtrado del cortafuego delimitará que usuarios acceden a los servicios internos y que tipo de acceso tienen. En el caso de la red inalámbrica, debido a la popularidad y seguridad que brinda en este sector, se ha utilizado el Portal Cautivo.

El Portal Cautivo es una técnica mediante la cual los clientes de la red necesitan forzosamente utilizar un cliente HTTP/HTTPS, o sea un navegador, para su autenticación antes de acceder al resto de los servicios internos de la red como es el caso de la navegación. Un Portal Cautivo convierte un Explorador Web en un dispositivo de autenticación, de modo que cuando se abre un explorador y se intenta acceder a un sitio web el usuario es redirigido a una página web que requiere autenticación, pago, o simplemente el consentimiento de las políticas de uso (netiqueta). Este tipo de mecanismo ha ganado mucha popularidad fundamentalmente en las redes inalámbricas (hoteles, centros comerciales, universidades, etc.) por las características peculiares de este tipo de red donde cualquiera con un dispositivo inalámbrico se puede conectar.

El funcionamiento es sencillo, esta tarea se realiza capturando todos los paquetes de red), independientemente del puerto, que llegan a la puerta de enlace (generalmente un cortafuegos hasta que el usuario trate de acceder a Internet, donde es redirigido a la página de autenticación. Luego de autenticado correctamente el usuario puede hacer uso del resto de los servicios que se brindan. Los mecanismos de autenticación en los portales pueden ser simples utilizando opciones como la de usuario y contraseña o algunas centralizadas como bases de datos de usuarios como pueden ser ldap, radius, etc.

Otra de las ventajas de los portales cautivos radica en el registro de sucesos, como los incidentes de acceso a la red, tanto los acertados como los fallidos, de modo que se puede tener control sobre los usuarios y direcciones IP que acceden diariamente a la red.

En el caso que ocupa se ha implementado el portal cautivo de pfSense, esto hace que cuando se trata de acceder a una web el portal redirige la petición a la dirección 192.168.3.1 en el puerto 8000 (**Fig. 2.24**). El mecanismo de autenticación utilizado es el más simple, mediante usuario y contraseñas locales en el cortafuegos, en la medida que este servicio se haga más extensivo se pueden mejorar estos mecanismos por otros más sofisticados y centralizados que brinda pfSense, como la autenticación por RADIUS [F].

Este servicio por defecto permitirá pasar todo el flujo de conectividad, o sea, el usuario autenticado tendrá acceso a todo el rango de puertos de servicios de red. Por esta razón será necesario como se comentaba anteriormente combinarlo con los filtros del cortafuego, de modo que solo se permita al usuario acceder a servicios como la web (HTTP/HTTPS), los servicios de correo (SMTP, POP3, IMAP) y a algún otro servicio puntual que se defina posteriormente.



Fig. 2.24 Página de recepción del Portal Cautivo ICM desde una navegador web.

#### 2.2.3.6. Concepción de la subred RAN.

En este epígrafe se hace referencia a la red de acceso remoto del Instituto Cubano de la Música. En esta red se ubican un conjunto de instituciones externas que pertenecen al sistema de la música. En respuesta a la necesidad de encontrar una solución a las limitaciones de conectividad que presentan estas entidades, se hace una propuesta teniendo en cuenta las diferentes posibilidades de conexión.

Otro de los propósitos radica en la conformación de una red primeramente provincial que pudiera ampliarse posteriormente al resto de las provincias conformada por las Instituciones de la Música, que permita el intercambio interno de información y servicios.

En esta red se tienen dos tipos de dependencia de cliente, los que se conectarán mediante enlace arrendado. Actualmente, en el instituto no se cuenta con la infraestructura tecnológica para dar soporte a este servicio pero se prevé hacer las coordinaciones con ETECSA (la empresa que ejecuta esos proyectos) para llevar a cabo esta tarea.

Por otro lado están los que pueden acceder desde la propia WAN de ENET usando la propia conectividad (enlace) con esta empresa, en este segundo caso tenemos actualmente un reducido grupo de instituciones que ya presentan la implementación técnica y que en algún momento se les estuvo brindando los servicios de conectividad, pero se dejó de utilizar pues se verificó que se compartía el canal, o sea el mismo ancho de banda, entre el flujo de Internet y el flujo de acceso a la red del instituto por parte de las instituciones externas. Además de que se desconocen los mecanismos de seguridad que soportan a esta transmisión de datos. La solución óptima para este servicio sería migrarlos a enlace arrendado, pues de lo contrario tomaría carácter obligatorio la ampliación del ancho de banda del canal.

#### 2.2.3.6.1. Conectividad mediante enlaces arrendados.

En el diseño de la topología de esta red, igualmente participa activamente pfSense siendo enrutador, cortafuegos y controlador de accesos. En el esquema de conectividad lógica participan varios de los modelos que se han visto hasta ahora.

Interfaces: VLAN		
Interface assignments	VLANs	
Interface	VLAN tag	Description
fxp0	2	ADSL1
fxp0	3	ADSL2
fxp0	4	ADSL3
fxp0	5	ADSL4
fxp0	6	ADSL5

**Note:**  
Not all drivers/NICs support 802.1Q VLAN tagging properly. On cards that do not explicitly support it, VLAN tagging will still work, but the reduced MTU may cause problems. See the pfSense handbook for information on supported cards.

Fig. 2.25 Esquema de subredes mediante VLANs en un servidor pfSense.

Para realizar esta configuración se puede utilizar, igualmente, el esquema de VLAN, de modo que con una misma interfaz de red en el cortafuego se pueda dar soporte a varias conexiones de acceso remoto, incluso es posible compartirla con la conexión de red inalámbrica que se había visto anteriormente. Claro está, este mecanismo, aunque en teoría no tiene limitaciones técnicas, en la práctica, solo se debe utilizar para un grupo de conexiones, según muchos expertos, de entre 4 y 8 conexiones por interfaz, por lo que, en caso de superar esta cifra, sería recomendable incorporar otra interfaz de red al sistema.

Utilizando el conmutador con soporte VLAN, se conecta en un puerto el cable que proviene del cortafuego identificándolo con todas las etiquetas de las VLAN correspondientes. Luego en el conmutador se conecta los modem-router e identificamos cada una de estas conexiones con una VLAN diferente dentro de las que configuramos en el cortafuego. En el otro extremo, o sea en las instituciones, no será necesario el proceso de identificación de VLAN, pues cada VLAN acaba en el modem-router correspondiente en el instituto.

La configuración tanto del conmutador como de los modem-routers va más allá de esta investigación por dos razones fundamentales, la primera se refiere a que no se cuenta aún en el Instituto con los dispositivos ni con la infraestructura técnica, como ya se había mencionado. La segunda proviene del hecho de que esto es solo un esbozo investigativo que se ha redactado basado en documentación práctica proveniente de la Internet. Es posible abundar más en este tema leyendo artículos [13a][13b] que aborden el tema.

Como se menciona el esquema de direccionamiento IP para estas conexiones utiliza direcciones privadas, pues escasean las direcciones públicas en el instituto. Cada puerta de enlace (interfaz VLAN en el cortafuego) tendrá la dirección IP 192.168.X0.1/24, donde X, por cuestiones de fácil identificación, será el identificador de la VLAN correspondiente, de este modo la VLAN2 en el cortafuego será la 192.168.20.1, usando este esquema de nomenclatura tendremos 24 (20-250) VLANs disponibles, y es poco probable que se conecten más de 24 instituciones, pero en tal caso se puede buscar alternativas pues realmente contamos con más de 250 subredes de clase C privada y otras tantas de Clase A y B.

Por otro lado están los modem-routers que requieren una dirección IP, o sea que les puede asignar la 192.168.X0.2 al modem-router interno y al modem-router externo la 192.168.X0.254, es decir que descontando estas tres direcciones, cada institución tendría 251 direcciones en la red RAN (WAN) del ICM.

Para la resolución de nombres de dominio estas redes pueden utilizar el DNS de reenvío que se mencionó anteriormente del cortafuegos o los DNS de la DMZ. Para la navegación y el acceso a otros servicios de red pueden utilizar un modelo semejante al de las redes internas que será explicado más adelante en este proyecto.

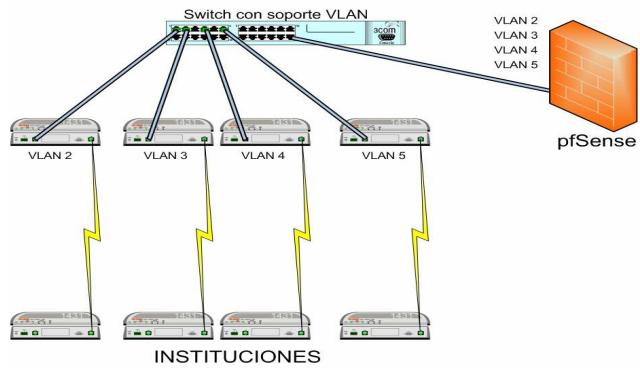


Fig. 2.26 Subredes mediante enlaces arrendados.

Fig. 2.26

### 2.2.3.6.2. Accesos desde la WAN por VPN.

Utilizando pfSense es posible implementar accesos remotos seguros a través de VPN. Una VPN (red privada virtual) es una red de computadoras en la que los enlaces entre los nodos son trasportados por conexiones abiertas o circuitos virtuales en algunas redes grandes (Ej. Internet), en lugar de hacerlo mediante conexiones cableadas, de modo que se aprovechan las ya existentes infraestructuras de conectividad. La capa de enlace del modelo TCP/IP en la VPN comunica a través de un túnel virtual que atraviesa otras redes extensas. La aplicación más usada de este concepto tecnológico está estrechamente asociada con la comunicación segura, pues a pesar de que el término no incorpora explícitamente las soluciones de seguridad como la autenticación y la encriptación del flujo, si ha servido de plataforma para la implementación de comunicaciones seguras, como la separación del tráfico de usuarios independientes (road-warriors) y comunidades (site-to-site) en el interior de otras redes menos seguras añadiendo a esta comunicación fuertes mecanismos de seguridad.

Utilizando pfSense es posible implementar accesos remotos seguros a través de VPN. Existen soluciones bien implementadas y probadas para este fin en el campo del software libre. Ejemplo de ello es la combinación de tecnologías como OpenVPN e IPSec.

Estas conexiones se pueden llevar a cabo tanto para entidades que se conectan a través de distintas redes, precisamente debido a que los mecanismos de enlaces se abstraen del tipo de conexión, tanto física como de enlace. Pudiera utilizarse en la WAN externa (WAN de ENET e Internet), poco confiable por naturaleza, o la WAN interna (RAN), que eventualmente pudiera llegar a no ser confiable en la medida que los enlaces pasan por una planta telefónica en la que se deposita la confianza sobre el flujo de información. Basado en este modelo se puede depositar más confianza en los accesos de las redes externas flexibilizando la seguridad entre estas y las redes internas.

Cabe destacar que en la versión actual liberada de pfSense, la 1.2, no se ofrece soporte para la conexión de usuarios individuales, debido a que tiene una implementación parcial para el soporte VPN. De esto, están más que claros, en el equipo de desarrollo y han prometido una solución completa para VPN en la versión 2.0 del producto, programada su lanzamiento, para finales de 2008.

Varios autores han redactado guías detalladas de configuración de VPN en pfSense, que encajan perfectamente con las necesidades en el instituto, por esta razón no se considera necesario mostrar el procedimiento completo, o sea, sólo se mencionan algunas de estas guías [F][14]. Además se ha encontrado sugerente referenciar otras guías alegóricas al tema; estas están enfocadas sobre sistemas software libre, en particular, sistemas operativos BSD actuando como clientes [15a][15b].

### 2.2.3.7. Mecanismos de seguridad de red en pfSense.

Existen dos tipos de políticas básicas en seguridad, de las que no quedan exentos los cortafuegos, restrictiva y permisiva. La primera se refiere a que todo está prohibido menos lo que está explícitamente permitido, la segunda opuestamente, permite todo lo que no esté explícitamente denegado. Las más común en redes, sobretodo empresariales, suele ser la restrictiva. La permisiva generalmente se usa en redes libres o en las primeras etapas de montaje del cortafuegos fundamentalmente para la organización y optimización de los mecanismos de filtrado.

En todos los diseños de redes basadas en cortafuegos, generalmente se fortalece la seguridad en el cortafuegos y se relaja un tanto en los host de las redes internas, principalmente en las redes de direcciones privadas. Por supuesto, esto no implica que estén totalmente desatendidas en cuanto a seguridad en la red, solo indica que no suele ser restrictivo el acceso a los servicios fundamentalmente a los que se brindan en otras redes conexas internas, siempre y cuando las políticas de la entidad lo permitan.

Sin embargo, en el cortafuegos la seguridad es el elemento primordial de ahí su función. Los cortafuegos modernos a diferencia de dispositivos con mecanismos de filtros como algunos enruteadores, trabajan en varias capas del los modelos de red TCP/IP, o sea, pueden ser más minuciosos en el filtrado del tráfico detectando por ejemplo los sistemas operativos y aplicaciones que generan dicho tráfico. Y como ventaja no solo detectan, sino que aplican acciones en determinadas incidencias de tráfico en correspondencia con la configuración que tenga.

Estos mecanismos se basan fundamentalmente en reglas de filtrado y proxies de aplicación. En esta sección se procede a explicar los mecanismos de comunicación entre las subredes que conformaran el conjunto topológico de la red del ICM. Se explican los esquemas de uso de los servicios dentro de un modelo seguro. Para implantar estos mecanismos será recomendable en todo momento seguir los patrones de seguridad impuestos tanto por las políticas de nuestra empresa, como por el propio diseño de red adoptado. Se buscara en todo momento el cumplimiento a cabalidad de muchas de las reglas básicas de seguridad.

#### 2.2.3.7.1. Las reglas del cortafuegos.

Los mecanismos de filtros en un cortafuegos se denominan reglas y rigen el tráfico que pasa a través de una interfaz (un conjunto de reglas por interfaz) de red del cortafuegos. El cortafuegos enrutará todos los paquetes que superan las barreras determinadas por las reglas en la interfaces y entran en el cortafuegos. Las reglas definen acciones que se ejecutan cuando un paquete cumple con los parámetros de la regla.

Las reglas se chequean en forma de lista consecutiva ordenada, o sea, un paquete es tratado por todas las reglas hasta que una explícitamente indica una acción a realizar con el paquete en cuestión. Respecto a esto es importante destacar que es muy importante prestar mucha atención al orden de las reglas, pues un ordenamiento apropiado de las reglas puede repercutir beneficiosamente tanto en la eficiencia como en la seguridad del cortafuegos.

Puede haber distintos tipos de acciones sobre los paquetes, las más simples solamente toman decisiones del tipo pasa, no pasa, en cuyo caso se puede bloquear el paquete sin notificación al emisor (*block o drop*) o con notificación o rebote (*reject*). Otros tipos de reglas registran (*log*) sucesos (muy útil para detectar intentos de violaciones tanto fallidas como satisfactorias o la generación de estadísticas de tráfico), otras reglas más sofisticadas modifican el contenido de los paquetes, entre estas reglas se encuentran las reglas de NAT (traducción de direcciones IP).

pfSense, como ya se había mencionado utiliza el programa cortafuegos *pf* originario de OpenBSD, considerado por muchos el más seguro de todos los cortafuegos por software. Está claro que realmente ningún software es seguro por si solo. Se habla de software seguro cuando brinda variadas y eficientes herramientas que le facilitan la implementación de la seguridad al administrador. *pf* lamentablemente no es el ejemplo más fiel de simplicidad en cortafuegos, aunque verdaderamente las herramientas están bien probadas por muchos especialistas ganando mucho prestigio. pfSense ha venido a salvarnos pues nos permite configurar muchas de las opciones de este cortafuegos de manera gráfica mediante la interfaz de administración web.

Una observación que se debe hacer cuando hablamos de la administración de sistemas cortafuegos, es que se debe tener mucho cuidado a la hora de ejecutar el cortafuegos sin antes ajustar correctamente las reglas pues nos puede dejar incomunicado con el exterior, situación en la que solo nos dejará acceder (si está permitido) a la PC localmente por la shell de comandos (menú en pfSense), no permitiendo (por ejemplo en pfSense) el acceso remoto (desde otra PC), ni por SSH, ni por el entorno de configuración web. En el caso debemos entendernos con el cortafuegos desde la propia consola por esta razón brindamos a continuación un conjunto de comandos de *pf* útiles para estos casos:

Comando	Función
<b>pfctl -d</b>	Deshabilita el funcionamiento de <i>pf</i>
<b>pfctl -e</b>	Habilita el funcionamiento de <i>pf</i>
<b>pfctl -f /etc/pf.conf</b>	Carga el fichero de configuración <i>/etc/pf.conf</i>

En pfSense el formato básico de una regla se divide en parámetros que serán chequeados en el paquete y la configuración de las acciones sobre en paquete en resumen sería (Fig. 2.27):

- *Acción*: Acción que ejecutará la regla en caso de hacer correspondencia con un paquete.
- *Interfaz*: Interfaz de red sobre la que se aplica la regla.
- *Protocolo*: Protocolo(s) a los que se aplica la regla, esto se refiere fundamentalmente a los diferentes protocolos de las distintas capas de la jerarquía TCP/IP (TCP, UDP, ICMP, IGMP, protocolos de aplicación, etc.).
- *Origen*: Computadora o red de la que proviene el paquete. Representadas por direcciones IP.
- *Puerto o rango Origen*: Desde qué puerto o rango de puertos fue emitido el paquete, existen un conjunto predefinido de puertos asociados con los protocolos de la capa de aplicación (HTTP, HTTPS, SMTP, POP3, etc.).
- *Puerto o rango Destino*: Similar a lo anterior pero referente al destinatario.

- *Registro del evento*: Registro en el log de sucesos, la incidencia de la aplicación de la acción al paquete.
- *Opciones avanzadas*: Fundamentalmente para restricciones sobre el flujo.
- *Estados*: esto se refiere a los estados<sup>5</sup> de comunicación entre aplicaciones de red.
- *Sincronización*: Mantiene esta regla sincronizada con otros cortafuegos en casos de redundancia de cortafuegos.
- *Horario*: Selección de los horarios en que se aplica esta regla.
- *Puerta de enlace*: Puerta de enlace que le dará salida al paquete, las puertas de enlace están asociadas a la configuración de rutas en el cortafuegos.
- *Descripción*: Campo de texto alegórico con el que se identifica la regla.

Una atractiva herramienta que nos brinda pfSense que nos resultará de gran utilidad, sobretodo al escribir las reglas del cortafuego es el empleo de *aliases*. Los aliases son palabras o frases que identifican, bien un conjunto de uno o más puertos de aplicación, un conjunto o subred de direcciones IP, etc. Con el uso de *aliases* se incrementa la flexibilidad de la configuración, pues se pueden hacer cambios más fácilmente, contando con el hecho de que los alias pueden conformar parámetros en las reglas del cortafuego. Los *aliases* definidos pueden emplearse o no, incluso se pueden definir *aliases* para utilizarlos en situaciones coyunturales. Los alias utilizados en reglas activas no se podrán eliminar.

---

<sup>5</sup> *Statefull firewall*: no todos los cortafuegos dan estas prestaciones. Pero es un mecanismo de sintonía bastante avanzado que requiere estudio profundo.

**Firewall: Rules: Edit**

Action	<input checked="" type="checkbox"/> Pass Choose what to do with packets that match the criteria specified below. <small>Note: the difference between block and reject is that with reject, a packet (TCP/RST or ICMP port unreachable for UDP) is returned to the sender, whereas with block the packet is dropped silently. In either case, the original packet is discarded. Reject only works when the protocol is set to either TCP or UDP (but not "TCP/UDP" below).</small>
Disabled	<input type="checkbox"/> Enable this rule <small>Set the option to disable this rule without removing it from the list.</small>
Interface	WAN <input type="checkbox"/> Choose on which interface packets must come in to match this rule.
Protocol	TCP <input type="checkbox"/> Choose which IP protocol this rule should match. <small>Note: in most cases, you should specify TCP here.</small>
Source	<input type="checkbox"/> not Use the option to invert the sense of the match. Type: any <input type="checkbox"/> Address: <input type="text"/>
Source port range	From: <input type="text"/> (other) <input type="checkbox"/> To: <input type="text"/> (other) <input type="checkbox"/> <small>Specify the port or port-range for the source of the packet for this rule. This is usually not equal to the destination port-range (and is often "any"). Hint: you can leave the To field empty if you only want to filter a single port. NOTE: you will not need to enter anything here in 99.99999% of the circumstances. If you're unsure, do not enter anything here.</small>
Source OS	OS Type: any <input type="checkbox"/> <small>Note: this only works for TCP rules.</small>
Destination	<input type="checkbox"/> not Use the option to invert the sense of the match. Type: any <input type="checkbox"/> Address: <input type="text"/>
Destination port range	From: <input type="text"/> (other) <input type="checkbox"/> To: <input type="text"/> (other) <input type="checkbox"/> <small>Specify the port or port-range for the destination of the packet for this rule. Hint: you can leave the To field empty if you only want to filter a single port.</small>
Log	<input type="checkbox"/> Log packets that are handled by this rule <small>Note: the firewall has limited log-space. Don't turn on logging for everything. If you want to do a lot of logging, consider using a remote logging server (see the Diagnostic System logs Settings page).</small>
Advanced Options	Simultaneous client connection limit: <input type="text"/> Maximum state entries per host: <input type="text"/> Maximum new connections / per second: <input type="text"/> State Timeout in seconds: <small>NOTE: Leave these fields blank to disable this feature.</small>
State Type	<input type="checkbox"/> keepalive <small>HINT: Select which type of state tracking mechanism you would like to use. If in doubt, use keep state.</small> <ul style="list-style-type: none"> <li><input type="radio"/> keep state      Works with all IP protocols.</li> <li><input type="radio"/> modstate state      Works early with TCP; packets will generate strong initial Sequence numbers (ISNs) for packets matching the rule.</li> <li><input type="radio"/> temporary state      Blocks incoming TCP connections to help protect servers from specified TCP SYN floods. This option includes the functionality of keep state and modstate state combined.</li> <li><input type="radio"/> none      It's not useful mechanisms to keep track. This is only useful if you're doing advanced queuing in certain situations. Please check the documentation.</li> </ul>
No XMLRPC Sync	<input type="checkbox"/> HINT: This prevents the rule from automatically syncing to other carp members.
Schedule	None <input type="checkbox"/> <small>Leave as 'None' to leave the rule enabled all the time. NOTE: schedule logic can be a bit different. Click here for more information.</small>
Gateway	default <input type="checkbox"/> <small>Leave as 'default' to use the system routing table. Or choose a gateway to utilize policy based routing.</small>
Description	<input type="text"/> <small>You may enter a description here for your reference (not parsed).</small>
<input type="button" value="Save"/> <input type="button" value="Cancel"/>	

Fig. 2.27 Configuración de una regla de cortafuegos.

Proto	Source	Port	Destination	Port	Gateway	Schedule	Description	Actions
<input checked="" type="checkbox"/> TCP	LAN net	*	YoursPC	*	*	*	Acceso completo a Red UPC	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>
<input checked="" type="checkbox"/> TCP	LAN net	*	CyberiaZonaCasa	*	*	*	Acceso completo a ZonaCasa ETG5	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>
<input checked="" type="checkbox"/> TCP/UDP	EDU-ETG5	*	*	*	*	*	Acceso completo para PC SETG5	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>
<input checked="" type="checkbox"/> TCP	*	*	ServiceSSH	22 (SSH)	*	*	Acceso a Servidores SSH	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>
<input checked="" type="checkbox"/> TCP	*	*	ServiceFTP	21 (FTP)	*	*	Acceso a Servidores FTP	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>
<input checked="" type="checkbox"/> TCP	*	*	ServiceWWW	80 (HTTP)	*	*	Acceso LAN > DMZ Servidores Web, MP, BD	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>
<input checked="" type="checkbox"/> TCP	*	*	ServiceEduCasa	PortaAltaBanda	*	*	Acceso a Lotus Lotus Doménico	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>
<input checked="" type="checkbox"/> TCP/UDP	LAN net	*	ServiceTerminalDMZ	3389 (MS RDP)	*	*	Acceso LAN a Servicios Terminal en DMZ	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>
<input checked="" type="checkbox"/> TCP/UDP	LAN net	*	ServiceEduCasaAlumnos	*	*	*	Acceso LAN a servicios de Alumnos en DMZ	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>
<input checked="" type="checkbox"/> TCP/UDP	*	*	1DMZ net	PortaBajaAccess	*	*	Acceso exterior ETG5, EDU	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>
<input checked="" type="checkbox"/> TCP/UDP	*	*	1DMZ net	PortaTHAccess	*	*	Acceso exterior ETG5, EDU/FTP/SSH	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>
<input checked="" type="checkbox"/> TCP/UDP	*	*	1DMZ net	PortaLotusDoménico	*	*	Acceso exterior ETG5, Lotus Doménico	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>
<input checked="" type="checkbox"/> TCP/UDP	*	*	1DMZ net	PortaMultimedia	*	*	Acceso exterior ETG5, Multimedia	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>
<input checked="" type="checkbox"/> TCP/UDP	*	*	1DMZ net	PortaHypervisorAlumnos	*	*	Acceso exterior ETG5, Hypervisor instant	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>
<input checked="" type="checkbox"/> TCP/UDP	*	*	1DMZ net	PortaTerminalAccessDSE	*	*	Acceso exterior ETG5, Terminal DSE	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>
<input checked="" type="checkbox"/> TCP/UDP	*	*	1DMZ net	PortaDSE	*	*	Acceso exterior ETG5, DSE	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>
<input checked="" type="checkbox"/> TCP/UDP	*	*	1DMZ net	PortaWWWAccess	*	*	Acceso exterior ETG5, web	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>
<input checked="" type="checkbox"/> TCP/UDP	*	*	1DMZ net	PortaAlumnosBandaFijaServices	*	*	Acceso exterior ETG5, Alumnos banda fija Services	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>
<input checked="" type="checkbox"/> TCP/UDP	*	*	ServiceExternos	*	*	*	Acceso completo a Servicios Externos a UPC	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>
<input type="checkbox"/> TCP	LAN net	*	UNIwired	*	*	*	LAN > Firewall DSE	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>

Fig. 2.28 Lista de reglas (filtros) en una interfaz de red..

### 2.2.3.7.2. Acceso desde la DMZ a la Internet.

La DMZ, como ya sabemos, es la sección pública de la red del Instituto, o sea la presencia en Internet por lo que, de acuerdo al criterio de los especialistas, es el área a la que mayor atención debemos prestar, por su importancia en cuestiones de seguridad. Es esta el área de mayor intercambio de tráfico con el exterior en la red completa, pues recordemos que existen otros mecanismos que generan, aunque en menor medida, intercambio de tráfico con el exterior como los dispositivos de almacenamiento extraíbles, ya que muchos son frecuentes portadores de virus que pueden infectar a los ordenadores de la red.

Otro elemento digno de recalcar es el hecho de que es en esta subred donde operan la mayoría de los servicios públicos hacia Internet por lo que se deben tener suma vigilancia sobre los flujos de comunicación en ambos sentidos. Debemos protegernos tanto de un ataque del exterior, como de que un atacante exitoso no utilice los servidores de la DMZ como plataforma para nuevos ataques, un ejemplo pudiera darse con el servidor de correo, para el envío de correo no deseado (spam) a otros servidores (la protección ante este tipo de ataque). Existen muchos más ejemplos de ataques [I], este que citamos es uno de los más simples y comunes.

Para mantener la comunicación entre la DMZ y el exterior se utiliza el modelo de cortafuegos transparente o pasarela de protocolos, pues recordemos que las direcciones IP en la DMZ son públicas, razón por la cual no es necesario utilizar otro modelo. El mismo consiste en añadir mecanismos de filtrado en el puente que previamente se añadió al cortafuegos. Mediante reglas de filtrado se permitirán estrictamente el paso de los paquetes que pertenecen a los protocolos de los servicios que se brindan en los servidores de la DMZ o que les estará permitido a estos acceder en el exterior.

Este modelo se denomina cortafuegos transparente (**transparent firewall**) debido a que: a los efectos, tanto de los servidores internos como los servidores externos (en la Internet), la presencia del cortafuegos es totalmente ignorada, ya que operan del mismo modo que suelen hacerlo cuando solo hay una ruta (conectividad) y no un cortafuegos de por medio. La presencia del cortafuegos solo se notará cuando desde alguna de las dos secciones se intente acceder a un servicio que tiene prohibido su paso por el cortafuegos, o sea, que no existe una regla que le permita pasar por el filtro habilitado puente (**filtering bridge**) DMZ. Un puente de filtrado en una combinación de un puente capa 2 (switch) y un filtro capa 3. En estas circunstancias los cortafuegos se desenvuelven de modo ad-hoc.

### 2.2.3.7.3. Acceso al exterior desde las redes internas.

En esencia, el acceso a servicios públicos en las redes internas se limita a uso de la navegación y el correo corporativo (estando en la DMZ a los efectos de las redes internas está en el exterior), pues el resto de los servicios, como los de almacenamiento y autenticación deben estar ubicados en el interior de las mismas.

Para la utilización de estos servicios, es vital el uso de la resolución de nombres de dominio (DNS). Para el acceso a este servicio, podemos habilitar esquemas de DNS de reenvío (forwarders), de los que se puede hacer uso tanto con los mecanismos que ofrece pfSense para esta tarea o configurarlos en algunos de los servidores internos con acceso a los DNS de la DMZ (este acceso se definiría mediante reglas en el cortafuegos).

Para el correo se puede hacer uso directo a los servidores en la DMZ, accediendo a los servicios de recepción y entrega SMTP, POP3 e IMAP en los caso indicados. De igual forma se puede habilitar el acceso al uso de la interfaz web de correo en cuyo caso se destinaría por los protocolos HTTP y/o HTTPS.

El resto de los servicios como navegación y FTP (en los casos que proceda, pues no se debe abusar del uso de este servicio por las repercusiones que tiene en el consumo de ancho de banda) se pueden habilitar mediante el uso de proxies de aplicación.

### **Proxies de Aplicación.**

En el contexto de las redes informáticas, el término **proxy** hace referencia a un programa o dispositivo que realiza una acción en representación de otro. Su finalidad más habitual es la de **servidor proxy**, que sirve para permitir el acceso a Internet a todos los equipos de una organización cuando sólo se puede disponer de un único equipo conectado, esto es, una única dirección IP (con acceso). Se debe enfatizar que el término "Internet" (que para los desconocedores se refiere sólo a la web) en realidad Internet abarca todo el espectro de protocolos de comunicación de aplicaciones bajo alguno de los modelos de redes como TCP/IP, los que son identificados lógicamente por puertos de protocolo de aplicación.

El uso más común es el de **servidor proxy**, que es un ordenador que intercepta las conexiones de red que un cliente hace a un servidor de destino. De ellos, los más famosos, básicamente por el tipo de uso que se le dan, son los **servidores proxy web** (comúnmente conocido solamente como «**proxy**»). Estos interceptan la navegación de los clientes por páginas web, por varios motivos posibles: seguridad, rendimiento, anonimato, etc. En la actualidad existen proxies de aplicación para casi cualquier protocolo y esto se ha logrado basándose en la amplia aceptación que han tenido. Por ejemplo existen proxies para otros protocolos, como el *proxy de FTP* y el *proxy de SMTP*. Existen algunos de capas de red más baja como el *proxy ARP* (utilizado en mecanismo de enrutamiento de redes).

El uso de proxies de aplicación tiene un conjunto de ventajas. En general los proxies brindan la posibilidad hacer tareas que anteriormente no se contaba con mecanismos para hacer:

- **Control.** Sólo el intermediario hace el trabajo real, por tanto se pueden limitar y restringir los derechos de los usuarios, y dar permisos sólo al proxy.
- **Ahorro.** Por tanto, sólo *uno* de los usuarios (el proxy) ha de estar equipado para hacer el trabajo real.

- **Velocidad.** Si varios clientes van a pedir el mismo recurso, el proxy mantener el recurso en caché, o sea guardar la respuesta de una petición para darla directamente cuando sea solicitada por otro usuario. Así no tiene que volver a contactar con el destino, y dando respuesta más rápido a la solicitud.
- **Filtrado.** El proxy puede negarse a responder algunas peticiones si detecta que están prohibidas.
- **Modificación.** Como intermediario que es, un proxy puede falsificar información, o modificarla siguiendo un algoritmo.
- **Anonimato.** Si todos los usuarios se identifican como uno sólo, es difícil que el recurso accedido pueda diferenciarlos. Pero esto puede ser malo, por ejemplo cuando hay que hacer necesariamente la identificación.

En cambio, no todo es perfecto en temas relacionados con proxies, existen algunas desventajas, el uso de un intermediario puede provocar:

- **Abuso.** Al estar dispuesto a recibir peticiones de muchos usuarios y responderlas, es posible que haga algún trabajo que no toque. Por tanto, ha de controlar quién tiene acceso y quién no a sus servicios, cosa que normalmente es muy difícil.
- **Carga.** Un proxy ha de hacer el trabajo de *muchos* usuarios.
- **Intromisión.** Es un paso más entre origen y destino, y algunos usuarios pueden no querer pasar por el proxy. Y menos si hace de caché y guarda copias de los datos.
- **Incoherencia.** Si hace de caché [16], es posible que se equivoque y dé una respuesta antigua cuando hay una más reciente en el recurso de destino.
- **Irregularidad.** El hecho de que el proxy represente a más de un usuario da problemas en muchos escenarios, en concreto los que presuponen una comunicación directa entre 1 emisor y 1 receptor TCP/IP [17].

En pfSense contamos con la disponibilidad de un conjunto de proxies soportados por el sistema y otros tantos se pueden añadir de alguna manera, pues recordemos que aunque pfSense todavía no soporta oficialmente la paquetería de FreeBSD puede añadir paquetes de forma equivalente a como se hace en el sistema que le dio origen, es decir que podemos de esta manera contar con la mayoría de los proxies que son soportados por FreeBSD.

La ventaja de usar los proxies soportados en pfSense, es que se pueden integrar al sistema, formando parte incluso de la interfaz de administración web. Esto nos facilita mucho la tarea de configurarlos. Ejemplo de ellos son, el Proxy web Squid y el FTP-proxy. De estos proxies nos podemos auxiliar para llevar algunos de los servicios públicos a las redes internas.

La navegación se resolvería, como decíamos, utilizando el proxy web Squid. En pfSense Squid se instala a base de clicks de la página de instalación de paquetes y posible combinarlo con otras aplicaciones afines, como el filtro de contenidos SquidGuard [18], que también son soportados por pfSense.

Realmente no es recomendable establecer una configuración muy sofisticada en este proxy, pues está alojado en el cortafuegos, o sea que no se debe sobrecargar con trabajo intenso ya que el cortafuegos enruta y filtra todo el tráfico de la red. Por esta razón, es más conveniente utilizar un esquema de proxies en cascada, utilizándolo fundamentalmente para aligerar el trabajo del host bastión, esta tecnología es a menudo utilizada en este tipo de situaciones. De esta manera se habilitan proxies en las redes internas que acceden al exterior usando el proxy central, delegando en ellos los mecanismos de autenticación y el intercambio con los usuarios finales. La sección de la seguridad en este proxy referente a la autenticación puede estar solo determinada por esquemas ligeros, quizás una combinación de direcciones MAC e IP y/o el uso de usuarios (proxies autenticados) de una base de datos local con su respectiva contraseñas, que pueden usar el resto de los proxies para autenticarse con el proxy central.



Fig. 2.29 Instalación del servidor proxy Squid en pfSense.

Otro proxy que pude resultar de utilidad en nuestra red en el proxy de FTP. El *FTP-Proxy Helper* como se le llama en pfSense, es una funcionalidad que *pf* brinda, donde la propia maquina (127.0.0.1) haga de proxy para las conexiones FTP. El hecho de contar con un proxy ftp en un cortafuegos es una ventaja pues el protocolo FTP suele ser complejo de configurar cuando se combina con un filtro de paquetes en un cortafuegos. Este proxy se habilita en la configuración de las interfaces que conectan a subred.

## 2.2.4. Otras prestaciones de pfSense.

Es posible notar con facilidad a lo largo de este capítulo el gran volumen de trabajo que se puede realizar tan solo apoyándose en un sistema tan completo como lo es pfSense, pero la cantidad de capacidades de pfSense está lejos de poder abarcarse en este trabajo. Todavía hay mucho que se puede hacer con pfSense, y a pesar de que las versiones actuales tienen implementaciones parciales y limitaciones con algunas herramientas, cuestión a la que ya se había hecho mención, los desarrolladores tienen una visión muy clara de lo que persiguen y en la medida que crece la aceptación y los requerimientos (que en ocasiones van acompañados de donaciones altruistas) por parte de los usuarios, más activa se torna la comunidad de desarrollo. Además al contrario de lo que muchos piensan respecto a la comunidad BSD, estos cuentan con todo el apoyo de los desarrolladores de sistemas afines como m0n0wall y en generar el resto de los desarrolladores BSD.

Finalmente hemos seleccionado un conjunto de características de pfSense que por su importancia no debemos pasar por alto, pues digamos que de alguna manera complementan este trabajo. No es intención, hacer con ellas un análisis profundo de su implementación, la idea es solo ponerlas en conocimiento de los lectores con el objetivo de que puedan ser encajadas luego en este y otros proyectos.

### 2.2.4.1. Alta disponibilidad y salva de la configuración.

En muchas redes, el cortafuegos es el único punto de fallo. Cuando el cortafuegos sale de funcionamiento, generalmente genera una catástrofe en la red completa, pues incomunica las redes internas entre ellas y con el exterior, razón de mucho peso por la que los especialistas han investigado soluciones para hacer frente a este tipo de eventos. En la actualidad se han implementado ya soluciones para este problema, basadas fundamentalmente en crear clústeres de cortafuegos en paralelo y sincronizados. La funcionalidad básica de esta prestación hace que todo el tráfico pase a través del primero mientras se encuentre funcionando normalmente (correctamente), en caso de fallo del cortafuegos primario, el cortafuegos secundario automáticamente (mecanismos de sincronía) comienza a tratar el tráfico, con lo que no se pierde la conectividad, todo continua funcionando como si nada hubiese pasado.

Esta configuración no solo incrementa la confiabilidad, beneficia también la seguridad consecuentemente. Por ejemplo, no es fácil actualizar el software del cortafuegos y probar la actualización sin que esto incida directamente sobre la red o sea sin sacar el cortafuegos de funcionamiento y lamentablemente actualizar el software del cortafuegos es vital, de esta manera se eliminan los agujeros de seguridad aplicando parches o instalando versiones nuevas.

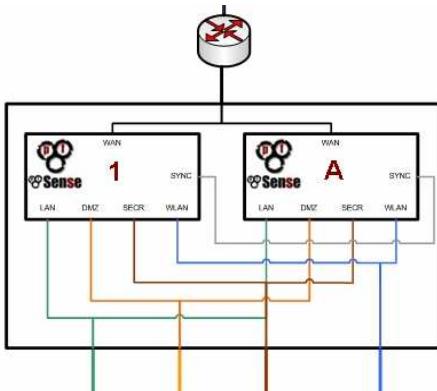


Fig. 2.30 Cluster pfSense de alta disponibilidad. que permite hacer clústeres de cortafuegos sincronizados [F].

Utilizando el esquema de cluster (**Fig. 2.30**), la tarea de actualización del software del cortafuegos se simplifica en gran medida, pues el cortafuegos secundario puede ser utilizado para estas cuestiones. Para probar desconectamos temporalmente el primario y comprobamos el rendimiento de las nuevas versiones.

pfSense ofrece una implementación originaria de OpenBSD que gestiona estas tareas de sincronización. Esta tecnología se basa en CARP (Common Address Redundancy Protocol) [19]

El CARP administra la prevención de fallos en la intersección de las capas 2 y 3 (enlace y red) del modelo OSI. Cada grupo CARP tiene un dirección MAC (enlace) virtual, y una o más direcciones IP (red) virtuales, que serán comunes en todo el grupo. El esquema de funcionamiento, radica en el envío de pines especiales vía multicast por parte del cortafuegos primario (master), estos mensajes utilizan el protocolo IP (puerto 112) como base y son recibidos por los servidores secundarios (backup). Cuando por algún motivo cesa en los secundarios la recepción (envío desde el primario) uno (contando con que pueden ser mas de uno) de los secundarios comienza el envío de estos mensajes tomando primacía.

Un segundo elemento significativo a la hora de brindar soporte de alta disponibilidad es el mecanismo de salva/recuperación de configuración que nos brinda pfSense. Esta tecnología nos permite hacer una salva íntegra de la configuración en un momento dado y la posibilidad de reestablecerla nuevamente en una sistema recién instalado o después de haber hecho cambios no consistentes en el sistema. Esta salva se mantiene en un fichero XML parametrizado que en todo momento se abstrae de las particularidades físicas (hardware) del cortafuegos haciéndolo compatible con otro equipo que no necesariamente tiene que ser idéntico. Este mecanismo puede ser utilizado en la implementación de alta disponibilidad por CARP, pues recordemos que estos equipos son equivalentes, solamente será necesario conectar correctamente los cable en la interfaces que corresponden.

Este mecanismo actualmente tiene un inconveniente, es posible salvar/recuperar toda la configuración que fue hecha utilizando la administración vía web, pero no brinda este soporte haciendo configuración desde la shell de comandos (recordemos que pfSense es un sistema BSD especializado), en cuyo caso no son reflejados en la interfaz de configuración web. En las ultimas versiones de pfSense viene incorporado un subshell php que nos ayuda a realizar esta tarea desde la consola, pero a pesar de que la idea es muy buena, aún no tiene la madurez necesaria para administrar todo el sistema, solo parte de la configuración básica. Por lo pronto la que se lleva a cabo desde la web funciona bien y podemos levantar un cortafuegos idénticamente al anterior después de un fallo o en un cluster.

#### 2.2.4.2. Publicación de servicios de redes internas.

Una de las necesidades que puede presentar cualquier entidad en un momento dado es la necesidad de publicar servicios de red que se ejecutan en las redes internas, los más comunes de estos servicios son la publicación web y el correo.

Por ejemplo en el ICM estos servicios se ejecutarán en la DMZ, que como se había hablado explicado es una sección pública de nuestra red con direcciones IP reales. Pero este caso desafortunadamente no es el más común, las direcciones IP reales escasean, y la posesión de uno de estos rangos en una empresa se puede considerar un privilegio, además estos rangos no alcanzan para repartir a todas las PC de la empresa.

Desde el mismo momento en que una entidad como el Instituto sostiene servicios de conectividad con algunas de sus dependencias, es señal de que se ha convertido en un proveedor de servicios de Internet (ISP) en alguna medida. Y un servicio completo consistiría en brindar además de la comunicación, la posibilidad de acceso desde el exterior a algunos de los servicios internos de estas dependencias, de este modo las instituciones pudieran administrar la publicación de algunos de sus servicios en la red de redes. Pero para esto necesita asignarle a las dependencias direcciones IP reales o adoptar algún otro mecanismo para lograr este efecto.

Podría ser también útil también hacer públicos algunos servicios de la red interna local quizás no a toda la Internet, pero si a la DMZ o a otras redes confiables en el exterior, asociados a estos pueden estar los servicios de salva (backup), registro de sucesos (log centralizados), algunos mecanismos de autenticación, etc.

El mecanismo que hace todo esto posible es denominado NAT (network address translation) en combinación con PAT (ports address translation). La traducción de direcciones de red. (Se conoce también como network masquerading o IP-masquerading). Consiste en reescribir las direcciones de origen y/o destino de los paquetes IP cuando estos pasan por un enrutador o un cortafuegos. Muchos sistemas usan NAT para que múltiples ordenadores o redes privadas puedan acceder a Internet usando una sola dirección pública. Los enrutadores no deberían hacer esto pero los administradores de red consideran esta una técnica adecuada y se usa ampliamente. Hay varios tipos de NAT:

- **Full cone NAT:** Todos los paquetes de la misma dirección y mismo puerto internos son mapeados a la misma dirección y mismo puerto externo. Cualquier host externo puede mandar un paquete al host interno mandándolo a la dirección y el puerto externo que ha sido mapeado. Se conoce como también como "one-to-one NAT". (NAT uno a uno).
- **Restricted cone NAT:** Todos los paquetes de la misma dirección y mismo puerto internos son mapeados a la misma dirección y mismo puerto externo. En este caso, en contraposición con full cone NAT, un host externo (con IP x.x.x.x) sólo puede mandar un paquete al host interno si previamente el host interno le había enviado un paquete a la dirección IP x.x.x.x.

- **Port restricted cone NAT:** es como restricted cone NAT, pero la restricción incluye también números de puerto. Un host externo (con IP x.x.x.x y puerto P) sólo puede mandar un paquete al host interno si previamente el host interno le había enviado un paquete a la dirección IP x.x.x.x y puerto P.
- **Symmetric NAT:** es NAT donde todas las peticiones de la misma IP y puerto interno con destino a otra IP y su correspondiente puerto son mapeadas en el enrutador con la misma IP y puerto. Si el mismo host interno manda un paquete con la misma dirección interna y puerto a un destino diferente se usará un mapeo diferente. Sólo el host externo que recibe un paquete puede mandar un paquete UDP de vuelta al host interno.

En pfSense existen mecanismos para dar soporte tanto para NAT (traducción de direcciones) para PAT (publicación de puertos). Esto se hace mediante direcciones IP virtuales, de modo que en cortafuegos puede haber tantas IP virtuales como servidores se quieran publicar al exterior, utilizándolas en las reglas de NAT. Las reglas de NAT en pfSense pueden publicar servicios (port forwarding) o servidores enteros (NAT 1:1) mapeados en hosts internos. También se puede configurar el NAT de salida (outbound NAT) que en esencia no es más que el network masquerading o IP-masquerading.

#### 2.2.4.3. Otros proxies de aplicación.

Se ha comentado ya sobre los proxies de aplicación, sin embargo, existen algunos proxies que cabe destacar aquí por su importancia, el primero de ellos es el filtro de clientes de chat (messengers) Inspector que viene como paquete soportado por pfSense. Este intercepta todo el flujo de clientes de mensajería instantánea, repudiado frecuentemente por su alto consumo de ancho de banda. Inspector trabaja mediante mecanismos de ACL o listas de acceso (whitelist), o sea se puede configurar para permitir el tráfico sólo a aquellos usuarios (contactos) que estén explícitamente en la lista de acceso, el resto sería denegado.

Otro proxy de aplicación que pudiera resultar interesante sobre todo en cuestiones de seguridad es el SMTP proxy. Los proxies SMTP en general son MTAs (Mail Transfer Agents) especializados que funcionan como el resto de los proxies de aplicación (no hacen todas las tareas de una MTA como relevo, almacenamiento y reenvío). La idea es que cuando reciben conexiones SMTP, abren otra conexión SMTP trasera (suponiendo que se instala en las puertas de enlace y cortafuegos) con los MTA destino. Y lo mismo en sentido contrario tanto para el envío como para la notificación de errores. En la paquetería de FreeBSD, por tanto instalables en pfSense (en la categoría SMTP solo soporta el proxy Spamd, un antispam ligero) existen algunos muy buenos. Uno que vale mencionar es el ASSP [20a][20b][20c]. ASSP es un Proxy SMTP orientado a pequeñas y medianas empresas. Preparado para ejecutarse ante sistemas que tengan alrededor de 300 usuarios y 100 000 masajes de correo diario.

#### 2.2.4.4. Registro de sucesos.

El registro de sucesos (logs) es una de las tareas vitales en cualquier sistema o servidor de producción. Gracias a estos registros se pueden almacenar y analizar una gran diversidad de parámetros de los sistemas que finamente se convierte en estadísticas de rendimiento en varios en varias líneas de análisis. En particular en los cortafuegos, por lo general las estadísticas y sucesos más importantes van ligados a la seguridad, al la conectividad y al rendimiento.

pfSense está preparado para ejecutarse en sistemas de muy bajos recursos, entre ellos los recursos de almacenamiento (disco duro, flash), de los que necesita muy poco (nada en el caso de live-CD). Por esta razón, no es prudente sobrecargar en sistema alojando los registros de sucesos en los propios sistemas. Afortunadamente en los sistemas UNIX en general, esto es una tarea que esta perfectamente articulada, existen sistemas como el syslog que se encarga de manejar las trazas de los sistemas de manera centralizada en el propio servidor, y más aún existen otros sistemas, que permite centralizar esta tarea a través de todos los equipos de la red, de modo que alojado en un servidor con buena capacidad de almacenamiento, puede gestionar de manera sincronía la generación de trazas de varios servidores (mediante tecnología cliente-servidor), estamos hablando del syslog-ng quien además se encarga de manera automática, de la rotación de logs (logrotate).

En pfSense, como es lógico, esta tecnología esta perfectamente encajada, de esta manera pfSense puede redireccionar todo el manejo de trazas a otro servidor. En el caso peor en que no contemos con sistemas de este tipo podemos añadir dispositivos de almacenamiento al cortafuego, en forma similar a como se hace en FreeBSD. Todo esto quiere decir que bajo ningún concepto debemos obviar esta tarea tan importante, pues la información que por esta vía se genera suele ser de mucho valor, pues con herramientas de comandos unix, como *vi*, *cat*, *grep* podemos encontrar casi cualquier cosa, incluso existen sistemas analizadores de logs que generan estadísticas y gráficos con información relevante.

#### 2.2.4.5. Monitorización.

El proceso de monitorización en pfSense es parte del sistema en sí. La interfaz Web de administración mantiene gráficos con información en tiempo real relativa a muchos parámetros como el rendimiento del hardware del equipo y el tráfico procesado, entre otros. pfSense dedica una entrada de menú para el chequeo del funcionamiento y rendimiento de los servicios del sistema desde el cual se puede acceder a los históricos por día, semana mes y año, de estadísticas de flujo y otras cuestiones. En el **Anexo I.A** se muestran algunas gráficas generadas por un cortafuegos pfSense en explotación.

El sector del monitoreo de sistemas y redes en software libre está representado por muy destacados exponentes. De ellos algunos se encuentran ya incluidos en el sistema de paquetes de pfSense:

- **NTOP** (Network TOP) es una herramienta que no puede faltar al administrador de red, porque permite monitorizar en tiempo real los usuarios y aplicaciones que están consumiendo recursos de red en un instante concreto y además es capaz de ayudarnos a la hora de detectar malas configuraciones de algún equipo (esto salta a la vista porque al lado del host sale un banderín amarillo o rojo, dependiendo si es un error leve o grave), o a nivel de servicio. Posee un microservidor web que permite que cualquier usuario, que sepa la clave, pueda ver la salida NTOP de forma remota con cualquier navegador, y además es GNU. El software esta desarrollado para plataformas Unix y Windows. En Modo Web, actúa como un servidor de Web, volcando en HTML el estado de la red. Viene con un recolector/emisor NetFlow/sFlow, una interfaz de cliente basada en HTTP para crear aplicaciones de monitoreo centradas en top, y RRD para almacenar persistentemente estadísticas de tráfico. Los protocolos que es capaz de monitorizar son: TCP/UDP/ICMP, (R)ARP, IPX, DLC, Decnet, AppleTalk, Netbios, y ya dentro de TCP/UDP es capaz de agruparlos por FTP, HTTP, DNS, Telnet, SMTP/POP/IMAP, SNMP, NFS, X11.
- **Nmap** es un programa de **código abierto** que sirve para efectuar rastreo de puertos TCP y UDP atribuido a Fyodor. Se usa para evaluar la seguridad de sistemas informáticos, así como para descubrir servicios o servidores en una red informática. Los administradores de sistema pueden utilizarlo para verificar la presencia de posibles aplicaciones no autorizadas ejecutándose en el servidor, así como los crakers pueden usarlo para descubrir objetivos potenciales. Nmap permite hacer el inventario y el mantenimiento del inventario de computadores de una red. Se puede usar entonces para auditar la seguridad de una red, mediante la identificación de todo nuevo servidor que se conecte: Nmap es a menudo confundido con herramientas para verificación de vulnerabilidades como Nessus. Nmap es difícilmente detectable, ha sido creado para evadir los Sistema de detección de intrusos (IDS) e interfiere lo menos posible con las operaciones normales de las redes y de las computadoras que son analizadas. Nmap puede funcionar en sistemas operativos como las diversas variables de Unix (Solaris, Mac OS X, y BSD), GNU/Linux y también en otros OS como Microsoft Windows y AmigaOS.
- **Snort** es el IDS (*Intrusion Detection System*) más conocido y completo. Un IDS es una herramienta que se engloba dentro de las aplicaciones de seguridad y que trata de monitorizar eventos sospechosos ocurridos en un sistema informático determinado. Dichos eventos tendrían como finalidad el compromiso de la seguridad del sistema auditado, lo cual puede evitarse si el sistema de detección funciona adecuadamente y está bien configurado. Snort es un *sniffer* de paquetes de red que se adapta a la perfección a la definición de un IDS. Snort descarga periódicamente un conjunto de reglas y en función del análisis de los contenidos de los paquetes genera una serie de alertas. El trabajo con IDSs suele ser muy ambiguo y flexible, pues estos generan muchas alertas, que en muchas ocasiones son falsos positivos, esto significa que no se deben sacar conclusiones precipitadas y bloquear conexiones válidas (con alertas) que realmente no incurren en peligro.

En cambio, pfSense todavía adolece de soporte para la integración de otros sistemas muy completos y reconocidos, pero no es de dudar que en versiones futuras esto sea solucionado progresivamente:

- **MRTG** (*Multi Router Traffic Grapher*) es una herramienta, escrita en C y Perl por Tobias Oetiker y Dave Rand, que se utiliza para supervisar la carga de tráfico de interfaces de red. MRTG genera un informe en formato HTML con gráficas que proveen una representación visual de la evolución del tráfico a lo largo del tiempo. Para recolectar la información del tráfico del dispositivo (habitualmente enrutadores) la herramienta utiliza el protocolo SNMP (Simple Network Management Protocol). Este protocolo proporciona la información en crudo de la cantidad de bytes que han pasado por ellos distinguiendo entre entrada y salida. Esta cantidad bruta deberá ser tratada adecuadamente para la generación de informes. También permite ejecutar cualquier tipo de aplicación en lugar de consultar un dispositivo SNMP. Esta aplicación proporciona como salida dos valores numéricos que se corresponden a la entrada y salida. Habitualmente suelen utilizarse scripts que monitorizan la máquina local.
- **Nagios** es un sistema de gran prestigio que trabaja en el monitoreo integral de la red y servidores. Monitoriza los hosts y servicios que se especifiquen, alertando cuando el comportamiento de la red no es el deseado y nuevamente cuando vuelve a su estado correcto. Originalmente su nombre fue Netsaint, Ethan Galstad lo creó y lo mantiene actualmente, junto con un grupo de desarrolladores de software que mantienen también varios complementos. Nagios fue originalmente diseñado para ser ejecutado en GNU/Linux, pero también se ejecuta bien en variantes de Unix. Nagios está licenciado bajo la GNU General Public License Version 2 publicada por la Free Software Foundation.

En el **Anexo I.B** se muestran algunas de las interfaces gráficas o de comando (en el caso de nmap) de las aplicaciones de monitoreo que se citan en estas listas.

# III

Guía de migración al software libre de los servicios de red.

### 3.1. Significado de la migración al software libre en el ICM.

Una vez que se ha remodelado el diseño de la red con el objetivo de eliminar un conjunto de carencias existentes en el modelo anterior y darle un mayor soporte a la seguridad integral en toda la red, no se ha querido desperdiciar esta oportunidad, en que se ha hecho un estudio minucioso y práctico del funcionamiento de los servicios de red y los sistemas que la componen, para encontrar una forma consistente de llevar a un nivel superior, no solo el esquema físico y lógico de la red, si no más allá, el esquema de funcionamiento en sí. Y no existe manera de lograr este salto cualitativo sin hacer un cambio radical en la maquinaria de procesamiento de nuestra red. De modo que, encontrar un complemento tecnológico rentable que permita encausar esta problemática, en los últimos años ha dejado de ser una tarea compleja. No más tenemos que observar las proyecciones del país y del mundo en general y automáticamente nos daremos cuenta, que la solución resalta ante nuestras narices.

No estamos hablando de otra, que de la migración al software libre. En estudio del rendimiento y funcionamiento, tanto de nuestra red como de escenarios equivalentes, se desprende la conclusión de que no existe mejor complemento para el nuevo diseño de la red, que un esquema seguro y duradero soportado sobre los sistemas de software libre. El software libre actual ha dado muestras de un alto nivel de madurez, robustez y seguridad. Se pueden citar cientos de exponentes, que con años de experiencia en su explotación que han logrado igualar y en muchos casos superar en aceptación los sistemas propietarios de código cerrado.

Realmente no es propósito de esta tesis enjuiciar ni desestimar a los sistemas propietario y de patentes, pues el desarrollo del software y la informática, en general, es el resultado del desarrollo mundial. Realmente detrás de cada sistema de cómputo está la entrega más o menos remunerada de especialistas con altos grados de conocimientos, muestra de ello, son los niveles de competitividad de cada uno de los sistemas que operan el mundo de la informática en los últimos tiempos.

Desafortunadamente, trazar un esquema de migración que valla más allá, de los servidores y servicios de red del instituto, llegando a cada PC y cada usuario es tarea compleja, al punto de que se ha dejado para una etapa posterior, pues ciertamente a nivel de país la migración (global) al software libre ocupa los primeros escaños en las prioridades de los centros rectores de las tecnologías de la información, por lo que cientos de especialistas están estudiando las formas menos invasivas de resolver esta problemática. Por esta y otras razones se ha decidido en esta segunda parte de la tesis, enfocarnos en objetivo de crear una guía metodológica de migración al software libre solo de los servidores y servicios de la red en general.

No es interés de este segundo módulo de la tesis, hacer un tratado detallado de la implementación de los sistemas en la red en cuestión, entre otras razones, por que esta guía se basa más en la investigación teórica, que en la puesta en práctica de estos sistemas en la red del instituto, pues si está claro que todos los sistemas que conforman esta guía han sido ya suficientemente probados y aceptados por la comunidad mundial de software libre.

Además esto es solo una guía que propone alternativas tanto de plataformas como aplicaciones a tomar en cuenta en una implantación real. En algunos casos en que se considera meritorio se hace un análisis bastante concreto, aunque sin profundizar en detalles técnicos, de lo que pudiera ser la implementación, esto realmente se hace para familiarizar a los lectores con las soluciones y convertirlos en potenciales candidatos a la migración en otras redes.

Es notable el carácter modular de esta tesis, y este capítulo no queda exento de esta concepción. La guía de migración ha sido dividida en partes lógicas complementarias: la adopción de un cortafuegos libre, elemento sumamente importante en redes empresariales, la migración de los servidores públicos (los que se alojan en la DMZ) y posteriormente los servidores de las redes internas. Se puede destacar que la mayoría de los sistemas aquí propuestos conforman estándares del software libre, esto quiere decir que no están atados a las plataformas que aquí proponemos.

A pesar de que la guía está, del algún modo, restringida a soluciones específicas y particulares de la red del ICM, subyacentemente es aplicable a otros entornos con distintos niveles de similaridad, además de que representa un (y quizás el primero) patrón en entidades bajo los modelos informáticos de la rama de la cultura, que desprende un conjunto de análisis y motiva a la creación de una guía migracional con carácter general dentro de la cultura y en el país en general.

### 3.2. Selección de los sistemas operativos libres.

Por cuestiones de uniformidad, se ha sido en extremo cuidadoso en la selección, en especial de las plataformas que sentaran las bases de esta guía, pues como es fácil de notar, el software libre es muy diverso y resultaría muy complejo trazar un esquema mixto (dentro de la variedad del software libre) de migración. Para esta guía se ha utilizado una familia de sistemas operativos libres, que son compatibles entre sí en gran medida y que como se verá su prestigio es intachable por sobradadas razones. Se podrá notar que la aplicabilidad de estos sistemas operativos va más allá de las fronteras de esta guía, por tanto de esta tesis. Se habla de los sistemas BSD, sistemas que con decenas de años de explotación han sido más que probados en entornos de producción, incluso con mayor nivel de responsabilidad que impuestos por la red del Instituto.

Las bases de una guía de migración, están soportadas fundamentalmente en la selección de uno o más sistemas operativos sobre los cuales se ejecutarán las aplicaciones seleccionadas. En este caso nuestra selección está enmarcada en el sector de los servidores de producción. Los servidores de producción son los servidores que soportan el conjunto de servicios que se brindan en una red, ejemplos de estos servicios sería, el correo corporativo, el acceso a navegación, la publicación web y otros tantos que pueden llegar a conformar una extensa lista. En ocasiones estos sistemas operativos son nombrados también como sistemas operativos de propósito general, pues muchos de ellos, pueden adaptarse a diferentes entornos de producción, incluso más allá del sector de los servidores, realmente esto es más común el mundo de los sistemas operativos UNIX-like, aunque cabe señalar que algunas distribuciones GNU/Linux como Ubuntu, han diferenciado las ramas de ediciones de servidor y ediciones de escritorio o usuario final.

### 3.2.1. Caracterización general de los BSD.

Según se había citado la selección está concebida dentro de la familia de los sistemas BSD y para entender las razones que fundamentan esta selección se ha preparado una extensa, pero consistente presentación de lo que representan estos sistemas en la que juega un papel protagónico uno de los más renombrados y antiguos (no quiere decir que viejo) de los sistemas BSD que hoy día operan, FreeBSD, pues la mayoría de sus atributos son compartidos con el resto de los integrantes de esta gran familia, donde algunos se han especializado en diversos sectores concretos como la seguridad y la portabilidad, y otros han pasado al bando de los sistemas propietarios, pero algo ha prevalecido, todos conservan su raíces en un ancestro común. Todo esto quiere decir que lo que se cumple para FreeBSD en cuestiones de sistemas operativos como eficiencia, rendimiento, disponibilidad, flexibilidad, robustez, portabilidad, seguridad y los demás términos alegóricos, también se cumplirá para el resto en proporciones equivalentes, haciendo salvedad en los que se han especializado en algunas de estas ramas, quienes por supuesto lo superan en alguna medida.

#### 3.2.1.1. ¿Qué es BSD?

BSD son las siglas de “Berkeley Software Distribution”. Así se llamó a las distribuciones de código fuente que se hicieron en la Universidad de Berkeley en California y que en origen eran extensiones del sistema operativo UNIX de AT&T Research. Varios proyectos de sistemas operativos de código abierto tienen su origen en una distribución de este código conocida como 4.4BSD-Lite. Añaden además un buen número de paquetes de otros proyectos de Código Abierto, incluyendo de forma destacada al proyecto GNU.

#### 3.2.1.2. Un poco de historia.

Durante la década de los 80 comienzan a surgir compañías que operaban en el mercado de las estaciones de trabajo. La mayoría optó por adquirir licencias de UNIX en lugar de desarrollar sistemas operativos ellos mismos. Cuando la propia AT&T fue autorizada para vender UNIX iniciaron una implementación un tanto rudimentaria llamada System III, seguida rápidamente por System V. El código base de System V no incluía capacidad de trabajo en redes, de manera que todas sus implementaciones habían de usar software de BSD, incluyendo TCP/IP, así como aplicaciones como la shell *csh* y el editor *vi*. En conjunto esas inclusiones fueron conocidas como las *Berkeley Extensions*.

Las cintas BSD contenían código fuente de AT&T y en consecuencia requerían una licencia de código UNIX. Hacia 1990 al CSRG (Computer Systems Research Group) se le retiraron los fondos y se enfrentó al cierre. Algunos de los miembros del grupo decidieron distribuir el código BSD, que era código abierto, sin el código propiedad de AT&T. Esta distribución de código respondió al nombre de *Networking Tape 2*, más conocida como *Net/2*. *Net/2* no era un sistema operativo completo: faltaba aproximadamente un 20% del código del kernel. Uno de los miembros del CSRG, William F. Jolitz, escribió el código restante y lo distribuyó a comienzos de 1992 como *386BSD*. Al mismo tiempo otro grupo de antiguos miembros del CSRG fundaron una empresa llamada *Berkeley Software Design Inc.* [21] y distribuyó una versión beta de un sistema operativo llamado *BSD/386*, que se basó en las mismas fuentes, quien finalmente pasó a denominarse *BSD/OS*. Esta rama continúa evolucionando, hoy día podemos encontrar servidores aún ejecutando versiones de este sistema [22a][22b].

*386BSD* jamás llegó a ser un sistema operativo estable, en lugar de ello dos proyectos surgen de él en 1993: *NetBSD* [23] y *FreeBSD* [24]. Ambos proyectos se conformaron gracias a la falta de paciencia que originó la espera de mejoras en *386BSD*. El proyecto *NetBSD* comenzó principios de año y la primera versión de *FreeBSD* no estuvo lista hasta finales de ese mismo año. En 1996 otro proyecto, *OpenBSD* [25], se separa de *NetBSD*.

### 3.2.1.3. Tipos de BSD.

La familia de los sistemas operativos libres BSD se ha conformado derivando de los tres máximos exponentes *FreeBSD*, *NetBSD* y *OpenBSD*, algo similar a lo que ocurrió en los sistemas Linux con *Debian*, *RedHat*<sup>6</sup> y *Suse*<sup>7</sup>. En cambio en los sistemas BSD no ha ocurrido esa explosión sobredimensionada de distribuciones, como es el caso de las cientos de distribuciones Linux que existen hoy día, de las que algunas, incluso, han abandonado la categoría de software libre.

Cada proyecto BSD mantiene su propio árbol de fuentes y su propio kernel. En la práctica, sin embargo, las diferencias en el entorno de usuario (“userland”) entre los distintos BSD son menores que las que hay entre las distribuciones GNU/Linux. Es difícil enumerar los objetivos de cada proyecto puesto que las diferencias son muy subjetivas. En general:

- **FreeBSD** tiene como meta ofrecer alto rendimiento y facilidad de uso al usuario final y es uno de los favoritos entre proveedores de contenidos web. Funciona en PC y en procesadores Alpha de Compaq. El proyecto FreeBSD cuenta con un número de usuarios significativamente mayor que los otros proyectos.
- **NetBSD** tiene como meta la Portabilidad: No en vano su lema es “of course it runs NetBSD” (que podría traducirse como “claro que funciona con NetBSD”). Funciona en máquinas que abarcan desde PDAs a grandes servidores e incluso ha sido usado por la NASA en misiones espaciales. Es una excelente elección para utilizar viejo hardware no Intel.

<sup>6</sup> Derivó en una edición propietaria, RedHat Enterprise, y una gratuita Fedora Core.

<sup>7</sup> Derivó en una edición propietaria, Suse, y una gratuita OpenSuse

- **OpenBSD** tiene como meta la seguridad y la integridad del código: combina el concepto de código abierto y una revisión rigurosa del código, que dan como fruto un sistema muy sólido, es frecuentemente elegido por instituciones preocupadas por la seguridad como bancos, entidades de cambio y departamentos gubernamentales de los EEUU. Al igual que NetBSD funciona en gran variedad de plataformas.

Hoy día, la familia BSD consiste, sumándole algunos activistas de Linux (*Ututo*, *Gentoo*, *Debian*, etc), en cinco ramas principales (tres de ellas gratuitas) con toda una variedad de distribuciones, quienes desde el 2001, cuando fue lanzada la última gran rama, *DragonFlyBSD* (basada en la serie release FreeBSD V4.x), *FreeBSD*, *OpenBSD*, *NetBSD* y *MacOS X* representan un nuevo brote de creatividad en el mundo de UNIX.

Los sistemas operativos BSD no son clones UNIX sino derivados de código abierto del sistema operativo de AT&T Research, el cual es a su vez ancestro del moderno UNIX System V. Por razones legales no pueden ser llamados como sistemas UNIX, pero es ampliamente aceptado que la familia BSD representa los UNIX de código abierto. Todos los sistemas BSD son compatibles con POSIX [26].

### 3.2.1.4. ¿Por qué los BSD no se conocen mejor?

Existen diversas razones por las que los sistemas BSD son relativamente desconocidos:

- En 1992 AT&T denunció a BSDI, el distribuidor de BSD/386, alegando que el producto contenía código propiedad de AT&T. El caso fue sobreseído en 1994 pero la huella del litigio perdura. Un detalle que el proceso judicial aclaró fue el de la nomenclatura: en los 80s BSD era conocido como “BSD UNIX”. Tras la eliminación del último vestigio de código de AT&T, BSD perdió el derecho a llamarse UNIX (es posible encontrar títulos de libros referentes a “*the 4.3BSD UNIX operating system*” y “*the 4.4BSD operating system*”). El traumatismo y la duración de este caso frenaron mucho el proceso publicitario de los sistemas BSD libres, aún en Marzo de 2000 un artículo publicado en la web aseguraba que el caso había sido resuelto cercano a la fecha.
- La mayor parte de la popularidad de Linux se debe a factores externos a los proyectos Linux, como las campañas publicitarias, en que las compañías que ofrecen servicios relacionados con Linux, invierten sumas de dinero sacando luego algún partido, hasta hace poco los BSD de fuente abierta carecían de tales defensores, pero esto está cambiando.
- Existe la creencia de que los proyectos BSD están fragmentados y enfrentados entre sí. El *Wall Street Journal* habló de la “balcanización”<sup>8</sup> de los proyectos BSD. Como en el caso del pleito, esa creencia se fundamenta en historia antigua y no perdura en nuestros días.
- Los desarrolladores de BSD, en general, suelen ser muy experimentados y ponen menos de su parte a la hora de hacer el sistema fácil de usar, priorizando otros atributos. Los recién llegados suelen sentirse más cómodos con Linux.

<sup>8</sup> El término surgió a raíz de los conflictos en la Península Balcánica ocurridos en el Siglo XX. La primera balcanización se dio en las guerras de los Balcanes y el término se reafirmó en las guerras yugoslavas. El término se usa también para describir otras formas de desintegración, incluyendo, por ejemplo, la subdivisión de la Internet en enclaves separados,<sup>2</sup> y la ruptura de acuerdos de cooperación debido al surgimiento de entidades competidoras enfascadas en luchas del tipo *beggar-my-neighbor* (fastidiar al vecino).

- Los desarrolladores de BSD con frecuencia están más interesados en depurar su código que en promocionarlo. El interés básico de los desarrolladores BSD, a diferencia de los de algunas distribuciones GNU/Linux, es que sus sistemas funcionen cada vez mejor (pues a pesar de que benefician a muchos trabajan para sí mismos) y que crezca la comunidad y la aceptación.

### 3.2.2. Presentación de FreeBSD.

En el mundo del software libre la palabra “*Linux*” suele ser utilizada como sinónimo de “*Sistema Operativo*” pero no es el único sistema operativo UNIX-like [27] libre. Existe un sistema operativo que ha sido caracterizado como “*The unknown giant among free operating systems.*”<sup>9</sup>[28] y no se habla de otro que de FreeBSD, quien para algunos siempre ha sido el sistema operativo que los sistemas basados en GNU/Linux han debido ser.

FreeBSD es un sistema operativo libre y tiene unos acuerdos de licencia también muy liberales, incluso más liberales [29] que las GNU/GPL. Se puede descargar FreeBSD libremente desde Internet. Pueden quemarse los CDs o comprar copias de FreeBSD de varias fuentes a precios muy asequibles. A diferencia de Windows, algunas versiones comerciales de UNIX y, por que no, de Linux, no existen diferentes tipos de licencia para usuarios o para servidores, para usos sin ánimos de lucro o comerciales (en cuyo caso puede devenir en el ahorro de grandes sumas de dinero solo en licencias), ni limitantes en la cantidad de máquinas en las que se puede instalar.

FreeBSD es código abierto. Esto significa que el código del sistema operativo completo está a disposición pública. Para los no programadores esto puede no tener mucho significado, sin embargo los usuarios finales son beneficiados del código abierto ya que miles de programadores usan FreeBSD. El hecho de que el código esté accesible para ellos permite que tanto los bugs como los posibles problemas de seguridad tengan una mayor probabilidad de ser detectados y erradicados prontamente que en los sistemas de código cerrado.

FreeBSD es usado por profesionales de la informática, estudiantes y usuarios particulares de todo el mundo en su trabajo, educación y ocio. Muchas grandes corporaciones le confían a FreeBSD su desempeño, entre las más renombradas se pueden citar a Sony, Yahoo!, Microsoft (¡Impresionante, no creen!), el proyecto Apache y los estudios de efectos especiales de Hollywood; se pueden ver mucho otros en FreeBSD Gallery [30].

---

<sup>9</sup> “El gigante desconocido entre sistemas operativos libres” <http://www.ibm.com/developerworksopensource/library/os-freebsd/>

### 3.2.2.1. FreeBSD y los sistemas operativos libres.

Mucho consideran que FreeBSD suele ser más estable que Linux, aunque esto en realidad puede tomar más efecto en el campo de los servidores de producción. Sin embargo, una gran limitación que presenta FreeBSD, es que, en presentar soporte para las más últimas tecnologías (en cuanto a dispositivos de hardware), a menudo suele ser más lento que Linux. Podemos añadir, en este aspecto, que el equipo de FreeBSD mantiene una lista actualizada de los controladores de dispositivos soportados para cada arquitectura, en particular para los servidores, existe un excelente soporte en el referente al hardware RAID, interfaces de red y de comunicación en general.

Cuando nos referimos a Linux hablamos solo del kernel (el sistema operativo es GNU/Linux), aunque distribuciones (Ej. RedHat, Debian, Suse y otras), brindan un instalador de las utilidades disponibles al usuario. Actualmente existen en lista [31] cerca de 300 distribuciones distintas, es cierto que esto brinda al usuario mayor flexibilidad en la selección, en cambio, dificulta el proceso de transferir las tecnologías de una distribución a otra. Las distribuciones no solo difieren en la facilidad de instalación y en la disponibilidad de las aplicaciones, en muchas ocasiones difieren también en la estructura de directorios, shells de comandos, entornos y manejadores de ventanas disponibles, en la instalación de software y los mecanismos de actualización y corrección de errores (patching).

FreeBSD es un sistema operativo completo (kernel + entorno de usuario), con una prestigiosa estructura heredada de las bases del desarrollo de UNIX. Tanto el kernel como las utilidades que provee son controladas por el mismo equipo de ingeniería, esto hace que sea menos propenso a las incompatibilidades de librerías. Las vulnerabilidades en la seguridad pueden ser rápidamente señaladas por el equipo de seguridad. Cuando nuevas utilidades o características del kernel son añadidas en una nueva versión, los usuarios simplemente necesitan leer un fichero, las notas de lanzamiento (RELEASE-notes), que se pone a disposición pública en la página principal del sitio de freebsd.org.

El manejo de paquetes en FreeBSD ha sido extremadamente optimizado. FreeBSD brinda dos mecanismos complementarios para la instalación de aplicaciones que no forman parte del sistemas base: el manejo de paquete que se encarga de la instalación de paquetes precompilados, semejante a como se hace en las distribuciones Linux (deb, rpm, etc); y el sistema de Ports, donde FreeBSD integra el manejo de paquetes y las actualizaciones desde Internet, de modo que nos permite localizar la fuente, descargarlo, compilarlo y generar el paquete binario de instalación en un proceso único. Por otra parte hay un repositorio central, un único lugar donde encontrar las fuentes del sistema operativo íntegro, incluyendo todas las versiones anteriores.

Algunas distribuciones GNU/Linux, entre las que vale destacar a Debian, tienen algunas características ventajosas similares a FreeBSD, como la de recordar la actualización de los paquetes; pero en opinión de algunos autores Debian (por tanto muchos de sus herederos) es un sistema que descansa sobre el kernel Linux accidentalmente, pues tanto el Hurd como los kernels BSD podrían brindarle un buen desempeño, muestra de ello son algunos de los proyectos relacionados que se llevan a cabo en el sitio de Debian.

Existe un conjunto de elementos que a pesar de tener equivalentes, en alguna medida, en los sistemas GNU/Linux no deja de ser importante su valoración a la hora de hacer la selección entre estos sistemas operativos libres. FreeBSD tiene muchas características notables. Algunas de ellas son:

- **Multiplataformismo** que le permite a FreeBSD ejecutarse en miles de plataformas de hardware entre las que podemos mencionar a *Intel x86 family (IA-32)*, computadoras compatibles con IBM PC otros como *DEC Alpha, Itanium, Sun UltraSPARC, IA-64, AMD64* para los que fue desarrollado como un sistema operativo de 64 bits desde sus inicios; y *PowerPC*, arquitecturas *NEC PC-9801* incluso ediciones de las *Microsoft's Xbox*. El soporte para nuevas arquitecturas está en constante desarrollo, por ejemplo arquitecturas como *ARM, MIPS* y *Niagara* de la SUN tienen soportes en distintos estados de implementación.
- **Multitarea expropiativa** con prioridades dinámicamente ajustadas para asegurar que distintas aplicaciones y usuarios comparten el ordenador de un modo equitativo, incluso bajo la mayor de las cargas.
- **Servicios multiusuario** que permiten a mucha gente usar un sistema FreeBSD simultáneamente para distintas cosas. Esto significa, por ejemplo, que los periféricos del sistema como impresoras y dispositivos de cinta son compartidos adecuadamente por varios usuarios del sistema o la red, y que pueden establecerse límites sobre recursos concretos para usuarios o grupos de usuarios, protegiendo los recursos críticos del sistema de un uso abusivo.
- **Conexión de redes TCP/IP** muy robusta (recordemos que fue justamente en los BSD donde nació esta tecnología), con soporte para estándares industriales como SLIP, PPP, NFS, DHCP, y NIS. Esto quiere decir que su máquina FreeBSD puede interoperar fácilmente con otros sistemas y hacer de servidor en una empresa, proporcionando importantes funciones como NFS (acceso a ficheros remotos) y servicios de correo electrónico, o poniendo a su organización en Internet con WWW, FTP, servicios de enruteado y cortafuegos.
- **Protección de memoria** que garantiza que las aplicaciones (o los usuarios) no pueden interferirse. Un error fatal en una aplicación no afecta al resto.
- **Entornos gráficos**, *X Window System (X11R6)*, estándar de la industria, provee a los usuarios una interfaz gráfica (GUI) por el coste de una tarjeta VGA y un monitor comunes, y viene con los fuentes completos.
- **Compatibilidad binaria** con muchos programas nativos de Linux, SCO, SVR4, BSDI y NetBSD.
- **Memoria virtual** diseñada con paginación bajo demanda y de la “caché unificada de VM/buffer” satisface a aplicaciones que requieren grandes cantidades de memoria de forma eficiente aún dando respuestas interactivas a otros usuarios.
- **SMP** Soporte para máquinas con múltiples CPUs [32].
- **Herramientas de desarrollo**, toda una colección aplicaciones para el desarrollo en *C, C++, Fortran, y Perl*. Muchos más lenguajes adicionales para investigación y desarrollo avanzados se encuentran también disponibles en la colección de Ports y paquetes.

- **Miles de aplicaciones** *listas para usarse o fáciles de portar* están disponibles en Internet. FreeBSD es compatible a nivel de código fuente con la mayoría de sistemas UNIX comerciales por tanto la mayoría de aplicaciones requieren muy pocos o ningún cambio para compilar.
- **Frameworks extensibles**, FreeBSD brinda un conjunto frameworks que nos permiten personalizar el entorno y manejar algunas necesidades puntuales. Se pueden citar algunos ejemplos de los mas importantes:
  - *Netgraph* es un sistema modular de interacción con redes que puede suplantar la infraestructura de trabajo con redes existente en el kernel. Una variedad de módulos operacionales son distribuidos con FreeBSD quienes incluyen soporte para *PPPoE*, *ATM*, *ISDN*, *Bluetooth*, *HDLC*, *EtherChannel*, *Frame Relay*, *L2TP*, solo por nombrar uno cuantos.
  - *GEOM* es un framework de transformación de lectura de disco modular. Es un sistema de capas de almacenamiento solapables (interconectables) que permite que nuevos sistemas de almacenamiento sean desarrolladas limpiamente e integradas al subsistema de almacenamiento de FreeBSD. Las versiones más modernas de GEOM proveen utilidades administrativas para usar los módulos existentes. Por ejemplo, utilizando este tecnología se puede crear imágenes de disco usando gmirror [33], crear un stripe usando gstripe [34] o crear dispositivo secreto compartido con gshsec [35].
  - *GBDE*, o Encriptación de Discos Basada en GEOM, nos facilita una potente protección criptográfica en los sistemas de fichero, dispositivos swap, y otros tipos de medios de almacenamiento. Además, GBDE encripta sistemas de ficheros enteros transparentemente, no sólo ficheros individuales. Una porción de texto plano nunca llega a los platos del disco.
  - *MAC*<sup>10</sup> [36] provee un acceso restringido a ficheros aumentando el sistema de permisos de acceso a fichero tradicional del sistema. Como MAC está implementado de forma modular, un sistema FreeBSD puede ser configurado para políticas variadas de sistemas de seguridad de grado militar.
  - *PAM*<sup>11</sup> [37], al igual que Linux, FreeBSD provee amplio soporte para PAM. Esto le oferta a los administradores un modelo de autenticación más sofisticado que el tradicional de username/password de los sistemas UNIX. También da la posibilidad de definir políticas para el control de la autenticación, como mero ejemplo se puede mejorar la calidad de la contraseña seleccionada por un usuario.

---

<sup>10</sup> Mandatory Access Control --> Control de Acceso Obligatorio.

<sup>11</sup> Pluggable Authentication Modules (PAM).

### 3.2.2.2. FreeBSD y la seguridad.

La seguridad es un aspecto que no pierde de vista el FreeBSD Release Engineering Team [38]. Esto se manifiesta en muchas áreas concretas:

- Todos los incidentes de seguridad así como sus correcciones son debidamente atendidos por el equipo de seguridad y son luego puestos a disposición de los usuarios como advertencias públicas. El equipo de seguridad tiene reputación por dar solución pronta a las cuestiones conocidas de seguridad.
- Toda la información relacionada con la seguridad y los procedimientos en su tratamiento en FreeBSD, así como donde encontrar más información sobre seguridad esta disponible en el sitio de FreeBSD [39].
- Uno de los problemas que acarrea el software de código abierto es el amplio volumen de aplicaciones a disposición. Hay literalmente decenas de miles de proyectos de aplicaciones de software libre cada uno con sus respectivos niveles de responsabilidad en los incidentes de seguridad. FreeBSD ha afrontado este reto con VuXML [40]. Todo el software distribuido en el sistema base de FreeBSD así como el software que se pone a disposición en la colección de Ports es comparada con una bases de datos de las vulnerabilidades conocidas. Los administradores pueden usar la herramienta portaudit [41] para determinar rápidamente si un software es vulnerable, y de serlo, se recibe una descripción del problema y una URL con información relativa extra.

Existen otros mecanismos en FreeBSD que le permiten a los administradores asegurar el sistema según las necesidades:

- La utilidad jail [42] permite la ejecución aislada de los procesos, es aplicable a cualquier aplicación, pero en especial es aconsejable a aquellas que no brindan un entorno chroot.
- Las herramientas chaflags [43] y las ACLs son originarias de FreeBSD y se utilizan para aumentar la seguridad de los permisos tradicionales de los sistemas UNIX. Pueden, por ejemplo, proteger algunos archivos de modo que no puedan ser modificados o eliminados ni por el superusuario root.
- FreeBSD ofrece 3 tipos de cortafuegos incorporados en el kernel que dan servicios NAT, esto como resultado da un nivel de flexibilidad a la hora de relacionar el nivel de seguridad, mediante reglas, más apropiado para un sistema.
- El kernel de FreeBSD es fácilmente modificable, de modo que un administrador puede despojarse de las funcionalidades que no necesita o que sólo necesita en determinadas circunstancias en cuyo caso puede hacer uso del soporte para carga de módulos del kernel por demanda en tiempo de ejecución siendo posible realizar esta tarea con utilidades que permiten la carga y descarga de los módulos así como ver los módulos cargados.
- El mecanismo de sysctl permite ajustar el sistema en tiempo de ejecución mediante cambios de estado en el kernel al vuelo sin necesidad de reiniciar el sistema.

### 3.2.2.3. Casos de uso de FreeBSD.

Debido a que FreeBSD es un sistema completo, libre y de código abierto que viene con un gran número de herramientas, entre ellas de programación, lo que se puede lograr con FreeBSD actualmente está sólo limitado por nuestra imaginación y nuestras habilidades como administrador de redes y sistemas y/o programador. Sin embargo, sin tener todo este conjunto de conocimientos o estudiando algo de estas disciplinas en la abundante y detallada bibliografía sobre temas relacionados y apoyándose quizás en alguna de las prestigiosas listas de correo o canales IRC, hay algunas cosas que se puedes hacer con FreeBSD en el campo de los servidores:

- Instalar un poderoso servidor Web o FTP.
- Instalar un eficiente servidor de correos.
- Un servidor DNS y de servicios de enrutamiento.
- Un servidor de ficheros o de impresión en entornos de redes Windows.
- Servidor de Bases de Datos y Salva y replicación.

Tal es la versatilidad y flexibilidad de FreeBSD que ha delegado en proyectos derivados en distintos niveles, son conocidos como los FreeBSD Flavors, con propósitos específicos algunos han tratado de mantenerse, dentro de lo posible, actualizados y compatibilizados con el sistema original:

- Sistemas de enrutamiento y cortafuegos: *m0n0wall* [44], *pfSense* [45].
- Sistema de almacenamiento y salva en redes: *FreeNAS* [46].
- Sistemas live-CD: *DesktopBSD* [47], *PC-BSD* [48], *TrueBSD* [49] *RoFreeSBIE* [50], *FreeSBIE* [51], *Frenzy* [52].
- Maletín de Herramientas de Administración Portable: *Frenzy* [52].
- Mini sistemas y sistemas ultraligeros: *Damn Small BSD* [53], *nanoBSD*, *TinyBSD*, *ThinBSD*
- Sistemas de telefonía VoIP: *AskoziaPBX* [54].

Pero FreeBSD no ha perdido de vista a los usuarios de escritorio, este puede servir perfectamente en estaciones de trabajo y portátiles. Brinda un eficiente soporte para el sistema X Windows donde tiene soporte para alrededor de 13 000 aplicaciones de terceros, incluyendo KDE, Gnomo y OpenOffice, con relativa facilidad para la instalación. Pero si aún no fuese suficiente existen como mencionábamos anteriormente distribuciones de instalación y entorno gráficos asequibles al usuario, entre las más destacadas están:

- ***DesktopBSD*** quien está enfocado en llevar la estabilidad y potencia de FreeBSD a los usuarios de escritorio. Internamente mantiene la misma estructura que su progenitor y los autores del proyecto alegan que no piensan hacer cambios en este sentido, con vistas a garantizar la robustez del sistema operativo así como la compatibilidad de los mismos.

- **PC-BSD** es un proyecto serio que está abogando en llevar la plataforma FreeBSD al los usuarios de escritorio de modo que se pueda llegar a obtener la facilidad y el ambiente agradable que ya tienen algunas distribuciones GNU/Linux, provee un instalador con GUI muy fácil de usar, y aunque se han hecho algunos cambios en la estructura del sistema, se mantiene lo más cerca posible de la línea de desarrollo de FreeBSD.
- **FreeSBIE** y **RoFreeSBIE** son proyectos similares orientados a los usuarios de escritorio pero optimizados para ejecutarse en entornos de live-CD eliminando la necesidad de instalar el sistema en el disco duro de la PC.

### 3.2.2.4. Ventajas en la adopción de soluciones FreeBSD.

El lector que ya ha leído hasta aquí está bien nutrido de la cantidad de ventajas en implicaciones favorables que puede tener la inserción de FreeBSD dentro de un marco informático dado. Hay una cuestión evidente: “Si no está roto no lo arregles”, si ya usa un sistema operativo libre de código abierto y está realmente satisfecho con él, probablemente puede no haber ninguna buena razón para cambiar. Pero la adopción de soluciones FreeBSD, y más como opción de migración al software libre, puede brindar un sinnúmero de ventajas:

- En general los sistemas BSD y en particular FreeBSD gozan de una mejor reputación en cuanto a disponibilidad, principalmente por la mayor madurez de su código base, es digno tener en cuenta que buena parte del código BSD data de más de 25 años de desarrollo y depuración.
- FreeBSD puede ejecutar<sup>12</sup> código de Linux, mientras que Linux no puede hacer lo propio con código de FreeBSD. Como resultado de esto hay una mayor cantidad de software disponible para FreeBSD que para Linux, sin notables diferencias en velocidad de ejecución entre una aplicación de Linux ejecutándose en un sistema Linux y una aplicación Linux ejecutándose en un sistema FreeBSD de la misma velocidad.
- FreeBSD es un sistema excelentemente documentado y sigue la mayoría de los estándares. Esto nos permite transferir fácilmente nuestros conocimientos y habilidades, si los tenemos claros, intermedios o avanzados en Linux y/o Unix a la administración en FreeBSD.
- La licencia FreeBSD nos permite modificar libremente el código, incluso cerrarlo, para ajustarlo al propósito de nuestro negocio. A diferencia de la GPL, no hay restricción en la forma que se escogerá para distribuir nuestro software.
- El modelo “todo del mismo proveedor” de FreeBSD implica que las actualizaciones son mucho más sencillas de gestionar de lo que con frecuencia son en Linux. FreeBSD maneja las actualizaciones de versiones de bibliotecas suministrando módulos de compatibilidad para versiones anteriores, de modo que es posible ejecutar binarios con varios años de antigüedad sin problemas.

---

<sup>12</sup> Dado que existen menos aplicaciones para BSD que para Linux los desarrolladores de BSD han creado un paquete de compatibilidad con Linux que permite hacer funcionar programas de Linux bajo BSD. El paquete contiene tanto modificaciones del kernel, con el fin de gestionar correctamente las llamadas al sistema de Linux, como ficheros necesarios para la compatibilidad con Linux como la Biblioteca C.

A manera de resumen es sugerente destacar que FreeBSD es un sistema UNIX-like maduro, que incluye un cuantioso número de buenas características de las que alguien pudiera esperar en un sistema UNIX. Para aquellos que desean unirse al movimiento de las soluciones libres de código abierto en alguna infraestructura informática, FreeBSD es más que una buena alternativa.

### 3.3. Migración de los servidores de producción de la DMZ.

Al llegar a este punto, se debe tener una noción bien clara de lo que son los sistemas BSD, y en particular los que prenden de la rama de FreeBSD. Ahora es ya momento de entender como operan estos prestigiosos sistemas operativos. El primer apunte que se hará es que esta sección no es más que la continuación de un trabajo ya comenzado, pues a todo aquel que no lo haya notado le hacemos la observación de que el capítulo 2 es exactamente lo que le faltaría a esta parte de la guía, que por razones más que obvias, se ha separado, dándole una atención especial y otro carácter aplicativo.

En esta sección de la guía se aborda la construcción de servidores de producción que brindaran servicios públicos bajo el sistema FreeBSD. En este caso es usada la más reciente versión estable, o sea la rama *STABLE* de la última versión FreeBSD 7.0. En los instantes en que se desarrolla esta tesis se prepara el próximo lanzamiento de la rama *RELEASE*, la versión 7.1, y se dan pasos agigantados en el desarrollo de la *CURRENT*, la muy prometedora versión 8.0, que debe estar lista para mediados del 2009.

### 3.3.1. Selección del hardware.

Como es de suponer, las nuevas modificaciones en el diseño de la red implican que la eficiencia en la prestación de los servicios debe también ser cualitativamente superior. Evidentemente esto no es posible lograrlo haciendo uso de hardware no profesional que no viene preparado para altos niveles de rendimiento y continuidad en el servicio. Por tal razón se ha decidido prestar seria atención a los requerimientos de hardware que se deben utilizar para dar soporte a servicios con tal grado de comprometimiento.

No es desconocido que, fundamentalmente a causa del bloqueo, encontrar en nuestro país tecnología de punta, especialmente en el campo de los servidores profesionales, se ha convertido

en una tarea difícil. Las comercializadoras de equipos informáticos se ven muy limitadas en las ofertas de este sector, quienes en ocasiones, buscando vías de solución, llegan a acuerdos con las instituciones clientes para adquisición de esta tecnología en el exterior, arreglo que nos es siempre factible, por disímiles cuestiones.



Fig 3.1 Servidor gama media Dell™ Poweredge™ 2900

Nuestra entidad, de alguna manera, ha sido afortunada en este aspecto, pues si bien, realmente no se ha podido hacer una selección minuciosa de los productos, se nos ha facilitado un tanto esta tarea con una de las proveedoras con la que se ha firmado contrato, la que nos ha hecho una oferta que se ajusta en una alto índice a los parámetros de nuestros requerimientos (teniendo en cuenta que la insatisfacción solo responde a la imposibilidad de selección), a raíz de una reciente adquisición de tecnología informática actualizada por su parte.

En esta oferta se han considerado para los servidores públicos dos servidores de gamma media: los Dell™ Poweredge™ 2900. En el **Anexo II.E** se puede apreciar la ficha técnica de estos equipos.

### 3.3.2. Implementación de los servidores.

Una vez que se tiene definida la arquitectura de hardware de los servidores que se van a montar en la DMZ, podemos dar paso a la confección de la guía para la instalación de los mismos. Será posible notar la estrecha similitud que existirá entre estos servidores, esto hace que se haya confeccionado una guía única, especificando las diferencias en el instante que proceda. Una porción de la guía que sigue será aplicable también a servidores en las redes internas, en consecuencia con la uniformidad de las plataformas adoptadas.

### 3.3.2.1. Instalación básica de FreeBSD.

FreeBSD ha preservado la manera antológica de instalación de los sistemas UNIX haciendo que la instalación [G][H] se haga en modo texto mediante una herramienta de mucha utilidad llamada *sysinstall*. Desde el mismo enfoque del sistema en sí, el instalador está orientado a personal con cierto nivel de habilidades, más preocupado por la correcta configuración y la flexibilidad que en una colorida y animada instalación gráfica. La herramienta *sysinstall* resulta de mucha utilidad no sólo en el proceso de instalación, sino posteriormente puede ser utilizado para cuestiones básicas de configuración y manejo de paquetes.



Fig. 3.2 Pantalla de inicio del sistema FreeBSD.

A pesar de su simplicidad, el instalador ofrece poderosas características semejantes a las que encontramos en los instaladores de las distribuciones GNU/Linux. Puede ser configurado para ser instalado desde diferentes medios locales CD, DVD o discos duros, o desde repositorios remotos vía HTTP, FTP o NFS. Además nos guía por diversas configuraciones como usuarios, servicios de red y muchas otras.

A continuación se muestra resumidamente el conjunto de pasos a seguir para realizar una instalación (desde CD/DVD) estándar de FreeBSD (este proceso suele ser análogo en las diferentes arquitecturas, la que se usa como patrón es la i386<sup>TM</sup>):

1. Si ya dispone de otro sistema operativo instalado, como Windows o Linux, puede usar los recursos que dicho o dichos sistemas operativos le faciliten para determinar exactamente que hardware tiene y cómo está configurado. Si tiene del todo claro qué configuración está usando, por ejemplo, una tarjeta de expansión concreta es posible que pueda encontrar esos datos impresos en la propia tarjeta.

2. Si la computadora en la que va a instalar FreeBSD contiene datos que desea conservar por algún motivo asegúrese de haber hecho una copia de seguridad de los mismos y de que esa copia es de fiar antes de instalar FreeBSD. El sistema de instalación de FreeBSD le mostrará una advertencia antes de modificar datos en su disco pero una vez que el proceso ha comenzado no hay manera de dar marcha atrás.
3. Insertamos el CD de FreeBSD en la disquera y reiniciamos el sistema. Por unos segundos aparecerá ante nosotros una pantalla de bienvenida, este tiempo puede ser abortado oprimiendo entrar.
4. Despues de arranque debemos seleccionar el país, y la distribución de teclado.

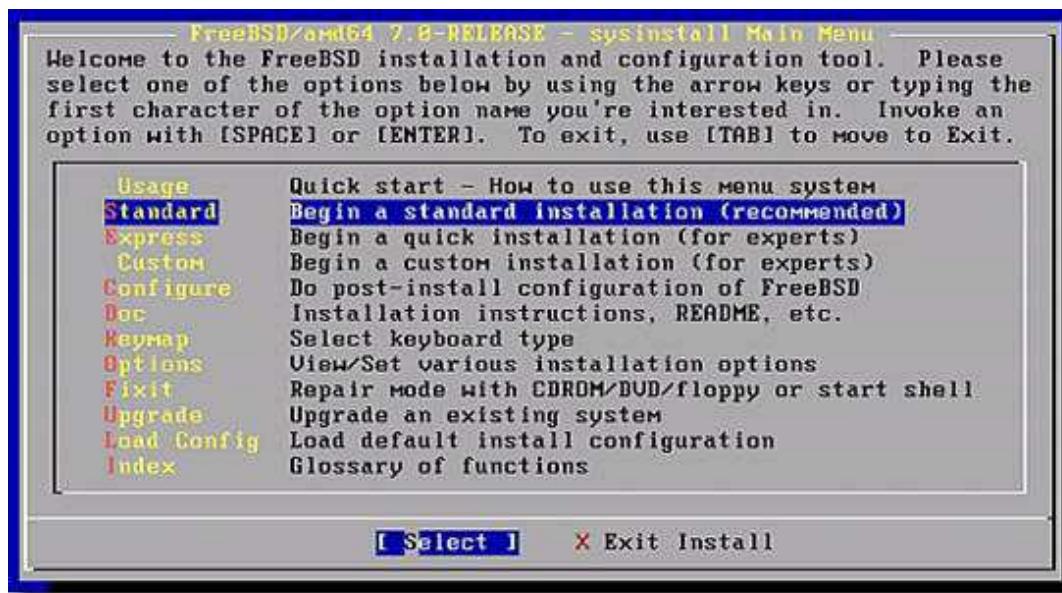


Fig. 3.3 Programa de instalación de FreeBSD, sysinstall.

5. Al momento estaremos frente al menú del *sysinstall*, donde escogemos la opción estándar (*Standard*) (Fig. 3.3).
6. Debemos ahora configurar los esquemas de particionamiento. Si se necesita que FreeBSD coexista con otros sistemas operativos tendrá que comprender cómo se almacenan los datos en el disco duro y como le afecta todo esto, en caso contrario seleccionamos las opciones por defecto (en lo adelante se asume que la PC será sólo para instalar FreeBSD).
7. La siguiente sección será la configuración del manejador de arranque. Se debería instalar el gestor de arranque de FreeBSD si:
  - a. Tiene más de un disco y ha instalado FreeBSD en un disco distinto del primero.
  - b. Ha instalado FreeBSD codo con codo con otro sistema operativo y quiere poder elegir si arrancar FreeBSD o ese otro sistema operativo cuando arranque su sistema.
8. Se continúa con el particionamiento de los discos (seleccionando las opciones por defecto).

9. Luego debemos seleccionar la distribución que vamos a instalar. Aquí frecuentemente, en la instalación de servidores, se selecciona la distribución minimal (a la que luego se le incorpora paquetería a nuestras necesidades). A continuación debemos indicar si deseamos instalar la colección de Ports (muy sugerente).
10. En la pantalla siguiente escogeremos el medio de instalación (en este caso CD /DVD).

En este instante nos encontraremos en un punto sin retorno en el que podemos abortar si no deseamos los cambios que van a ocurrir en el (los) disco(s) duro(s), caso de aceptar procederá la instalación, la que tomará un tiempo que dependerá fundamentalmente de la distribución que haya elegido, el medio de instalación y la velocidad del sistema.

Luego viene una segunda etapa, donde podemos configurar nuestro servidor según los parámetros que correspondan a sus configuraciones básicas, después del diálogo de felicitaciones por la instalación satisfactoria, pasamos a configurar:

1. Los dispositivos de red:
  - a. IPv6 (este no es nuestro caso),
  - b. configuración por DHCP que, en caso de seleccionarla debemos poner el nombre (FQDN) del host, en otro caso debemos asignarle una configuración estática.
2. Servidor como puerta de enlace (“gateway”).
3. Los de servicios de Internet.
  - a. Superdemonio inetd.
  - b. Acceso SSH.
  - c. Servidor FTP anónimo.
  - d. Servidor NSF.
  - e. El cliente NFS.
4. El Perfil de seguridad (conjunto de opciones de configuración que intenta suministrar el grado de seguridad deseado activando y desactivando ciertos programas)
5. Las consolas virtuales del sistema.
6. La zona horaria.
7. Habilitar la compatibilidad binaria con Linux.
8. La configuración del ratón (mouse) de consola. (Esta opción le permitirá cortar y pegar texto en consola y en otros programas mediante un ratón de tres botones.)
9. Servicios adicionales de red.
  - a. Selección del MTA por defecto
10. Instalación de paquetes (a menos de estar seguro de lo que se hace, normalmente esto no se hace en esta etapa).
11. Las cuentas de usuarios y grupos que accederán al sistema (los usuarios que podrán tomar los privilegios del superusuario root mediante el comando *su*, necesitarán formar parte del grupo *wheel*).
12. La contraseña del superusuario root.

Finalmente el *sysinstall* nos preguntará si queremos configurar algo más, donde si rechazamos, nos llevará al menú principal, de modo que al salir del mismo el sistema debe reiniciar. A partir de este instante el sistema ya está instalado y se ha realizado la configuración básica. Ahora el sistema está listo para ser administrado, apareciendo el prompt de acceso, donde damos nuestro usuario y contraseña y accedemos al sistema.

Una tarea común que es muy recomendada en los sistemas recién instalados es la actualización del sistema. Para hacerlo será necesario estar conectado a Internet o, al menos, tener acceso a un repositorio de FreeBSD con la actualización más fresca posible. Es sumamente importante mantener el sistema actualizado, esto nos mantendrá libre de agujeros de seguridad, errores de programas y al mismo tiempo el sistema permanece disponible, reiniciando sólo cuando se termina de ejecutar la actualización completa. La actualización total o parcial no está restringida a los sistemas recién instalados, esta, realmente, es una tarea que se puede hacer esporádicamente (mientras más frecuente se hace más compatibles son las nuevas actualizaciones). Además las tareas de actualización adecuan la instalación al hardware de nuestro servidor.

Actualizar el sistema requiere, primeramente, actualizar, las fuentes del sistema, compilar algunas (incluso todas) partes como librerías, el kernel y otras, a tal punto de que los más profesionales pueden modificar a su gusto el código, alterando los binarios que van a ser generados ajustándolos a sus preferencias y ganando en rendimiento. Existe también formas de actualizar obviando el proceso de compilación, para aquellos que no se quieren complicar ejecutando actualizaciones binarias.

Tanto para los desarrolladores como para los usuarios finales, todas las fuentes están accesibles de los CVSs del proyecto. Pero esto conlleva que los administradores de sistema deben tener conocimientos básicos de CVS (sistema de versiones concurrentes), estos son usados por los desarrolladores, para almacenar las fuentes separadas cronológicamente, donde los usuarios pueden mantenerse al día con las últimas actualizaciones.

Existen diversas maneras de administrar las actualizaciones, fundamentalmente las que están relacionadas con la seguridad. Algunas de ellas son:

- La compilación del *kernel* y el *World*, se actualiza mediante compilación el sistema base de forma íntegra.
- CVSup, mecanismo que sincroniza las fuentes del sistema con los CVS centrales.
- Actualización de la colección de Ports, la herramienta *portaudit* suele ser muy útil en cuestiones de seguridad, pues nos mantiene avisados de las incidencias relacionadas con los Ports, antes de instalarlos.
- Actualizaciones binarias.
- Recuperación ante *kernel* corrupto.

### 3.3.2.2. Servidores DNS del dominio *icm.cu*.

La resolución de nombres de dominio (DNS), definido por el RFC 1035 (y otro conjunto RFCs que introducen mejoras y extensiones), es uno de los protocolos que hacen funcionar el engranaje de la Internet, haciéndonos más sencilla su utilización mediante el establecimiento de correspondencias entre direcciones IP (difíciles de memorizar) y nombres. Por ejemplo una consulta preguntando por *www.icm.cu* recibe una respuesta con la dirección IP del servidor Web de nuestro instituto, mientras que una pregunta sobre *ftp.icm.cu* recibe como respuesta la dirección IP correspondiente al servidor de FTP. El proceso inverso sucede de una forma similar. Una pregunta relativa a una determinada dirección IP se resuelve al nombre de la máquina que la posee. No se necesita ejecutar un servidor de DNS para poder realizar consultas y búsquedas de DNS.

A pesar de parecer una tarea tan simple, DNS ha evolucionado desde su creación en 1983, ganando en complejidad y en prestaciones (hoy día algunos servidores DNS son capaces de hacer esta traducción con números telefónicos usando la extensión ENUM, por sólo citar un ejemplo). El DNS se coordina de forma distribuida a través de Internet donde un grupo de servidores de nombres representan las zonas raíces con autoridad sobre otras zonas y otro grupo de servidores de nombres de menor escala que se encargan de administrar o replicar la información de dominios individuales con el objetivo de mejorar los tiempos de respuesta de búsquedas reiteradas de la misma información.

FreeBSD 7.0 utiliza por defecto la versión 9.4.2 de BIND (Berkeley Internet Name Domain) de la serie 9.4 que ofrece las últimas mejoras en cuanto a rendimiento y seguridad [G], y soporte para IPv6 y DNSSEC. BIND puede ser usado en los modos de funcionamientos de los DNS.

En el modo Autoritativo (Authoritative), BIND mantiene en disco los ficheros con información sobre las zonas y responde las consultas basadas en la información local. Este a su vez se divide en dos subtipos, servidor maestro o primario será el servidor DNS donde se realizan las tareas de administración de la información de los dominios que sirve; servidor esclavo o secundario es el que mantiene un réplica sincronizada con el servidor primario, las funciones principales serán como servidor de respaldo del primario (responderá si el primario no lo hace) y como balance de carga para no sobrecargar el servidor maestro.

En modo caché de relevo (caching forwarder), BIND no mantiene información de dominios local, a cambio redirige las consultas a otros servidores DNS especificados o a los servidores raíces (root DNS servers) y estas repuestas las mantiene temporalmente guardadas en el caché para consultas similares. Estos suelen ser utilizados como mecanismo de seguridad en cortafuegos para proteger los servidores primarios, siendo el cortafuego quien atiende las consultas DNS de las redes externas.

## Instalación y configuración los servidores DNS.

La primera tarea será chequear si la versión del Port supera a la 9.4.2 (versión ya instalada en el sistema base), pues de lo contrario no será necesario instalar nuevamente:

```
# cat /usr/ports/dns/bind94/Makefile | grep PORTVERSION
```

Si se decide instalar el sistema, entonces se puede utilizar los comandos:

```
# cd /usr/ports/dns/bind94
# cd make configure ; make clean
```

Aparecerá un menú donde se debe marcar la opción REPLACE\_BASE para reemplazar el que viene instalado por defecto. Luego se debe añadir una línea al fichero `/etc/make.conf`, esto sería:

```
# cp /etc/make.conf /etc/make.conf.old
# echo 'NO_BIND="YES"' >> /etc/make.conf
```

Esto permite que en una posible actualización del sistema recompilando el sistema base, no sea sustituido el servidor DNS que está instalado por el que instala el sistema por defecto. Ahora se puede editar los ficheros de configuración para configurar las zonas:

```
# cd /var/named/etc/namedb/
# cp named.conf named.conf.old
# ee named.conf
```

Para permitir que el BIND atienda las solicitudes provenientes desde todas la interfaces de red se debe comentar e liminar la línea:

```
// listen-on      { 127,0,0,1 };
```

Para configurar los preenvíos (forwarders) se debe descomentar la sección correspondiente y reemplazamos la dirección local por los servidores relevos:

```
forwarders {
    200.55.128.4; 200.55.128.3;
};
```

La configuración de las zona(s) de búsqueda delantera y de búsqueda inversa en el servidor maestro podrían quedar semejante a:

```
zone "icm.cu" {
    type master;
    file "master/icm.cu.zone";
    allow-transfer { localhost; 200.55.136.172; };
    notify yes;
    allow-update { key rndc-key };
};
```

```
zone "136.55.200.in-addr.arpa" {
    type master;
    file "master/icm.cu.rev";
    allow-transfer { localhost; 200.55.136.172; };
    notify yes;

    allow-update { key rndc-key };
};
```

En el caso del servidor esclavo o secundario sería:

```
zone "icm.cu" {
    type slave;
    file "slave/icm.cu.zone";
    masters { 200.55.136.171 };
};
```

```
zone "136.55.200.in-addr.arpa" {
    type slave;
    file "slave/icm.cu.rev";
    masters { 200.55.136.171 };
};
```

Ahora es necesario añadir el fichero *rndc.key* (el mismo para ambos servidores) al contenido del fichero *named.conf*, el fichero *rndc.key* es la llave utilizada por la utilidad *rndc* para hacer su función de control sobre el servidor DNS, para esto se pueden utilizar los comandos:

```
# rndc-confgen -a
# cd /var/named/etc/namedb
# cat rndc.key >> named.conf
```

Con esto se termina de configurar el fichero *named.conf*, ahora resta hacer los cambios en los ficheros de zona *icm.cu.zone* y *icm.cu.rev*:

```
# cd /var/named/etc/namedb/master
# ee icm.cu.zone
# ee icm.cu.rev
```

Evidentemente será necesario añadir algunas otras entradas, pero a grandes rasgos estas serían versiones resumidas de los ficheros de zona delantero e inverso respectivamente:

```
$TTL 3600
icm.cu.           IN  SOA ns1.icm.cu.  root.icm.cu. (
                    1      ; Serial
                   10800   ; Refresh
                     3600   ; Retry
                   604800  ; Expire
                  86400 ) ; Minimum TTL
; DNS Servers
@                 IN  NS   ns1.icm.cu.
@                 IN  NS   ns2.icm.cu.

; Mail MX Records
@                 IN  MX   10   mail.icm.cu.

; Computer names and records
aramis.icm.cu.    IN  A    200.55.136.171
dartagnan.icm.cu. IN  A    200.55.136.172

; Aliases
ns1               IN  CNAME aramis.icm.cu.
ns2               IN  CNAME dartagnan.icm.cu.
mail              IN  CNAME dartagnan.icm.cu.
www               IN  CNAME aramis.icm.cu.
```

```
$TTL 3600
136.55.200.in-addr.arpa.  IN  SOA ns1.icm.cu.  root.icm.cu. (
                    1      ; Serial
                   10800   ; Refresh
                     3600   ; Retry
                   604800  ; Expire
                  86400 ) ; Minimum TTL
; DNS Servers
@                 IN  NS   ns1.icm.cu.
@                 IN  NS   ns2.icm.cu.

; Computer IPs
171              IN  PTR  aramis.icm.cu.
171              IN  PTR  ns1.icm.cu.
171              IN  PTR  www.icm.cu.
172              IN  PTR  dartagnan.icm.cu.
172              IN  PTR  ns2.icm.cu.
172              IN  PTR  mail.icm.cu.
```

Un vez instalado y configurado el DNS, solo restará arrancar el servicio. Para esto es necesario añadir una línea en el fichero `/etc/rc.conf`, para luego arrancar el servicio:

```
# echo 'named_enable="YES"' >> /etc/rc.conf
# /etc/rc.d/named start
```

### 3.3.2.3. Servidor Web, FTP y Bases de datos.

La publicación de contenidos en la Internet se ha convertido en un elemento de vital importancia para cualquier empresa, independientemente de su tamaño y función. Hay en Internet muchísima información de toda clase y aún queda mucho por publicar, pues empresas como el Instituto Cubano de la Música son fuente inagotable de contenidos e información de mucho interés, incluso a nivel mundial, son entidades con está las encargadas de enseñar al mundo los valores culturales de la sociedad cubana. Por esta razón se hace imprescindible la presencia de un servidor web eficiente mediante el cual se gestione esta tarea. Existen buenos candidatos en el software libre; su excelencia, calidad de servicios, robustez y estabilidad hacen que día a día empresas y administradores reiteren su confianza y renueven la elección a este servicio en plataformas libres. Una tendencia muy fuerte en el mercado de Internet ha sido marcada, la construcción de páginas web, el concepto de la definición de la Web 2.0, el desarrollo masivo de aplicaciones libres y por sobre todas las cosas la difusión de una comunidad atraída por una filosofía. En estos últimos años, estadísticas muy favorables apuntan a un uso extendido de estas aplicaciones, la gran mayoría de los servidores que encontramos en Internet utilizan servidores gratuitos, nuevamente mostrando el éxito de un software que por sobre todas las cosas es software libre, código abierto.

Otro servicio que frecuentemente acompaña al servidor web es el servicio de FTP. Es muy usual esta combinación cuando se ofrecen servicios de hosting (publicación web administrada por el usuario), pues en este caso es el servidor web el que se usa para subir los contenidos al servidor. Pero brindar servicio FTP no es una tarea que se debe tomar a la ligera, pues por ejemplo el servicio FTP que viene disponible en el sistema base de FreeBSD realmente no está diseñado para dar servicio público y menos en el caso de un servidor web expuesto a los riesgos que atentan contra un servidor público en la DMZ y que pueda brindar mecanismos para que los webmasters (administradores de sitios) controlen sus contenidos usando este servicio. Representa un gran problema de seguridad el intercambio de información con mecanismos de texto plano, pues todos los datos (incluyendo las contraseñas) viajan a través de la red sin encriptar, de manera que cualquiera con acceso al canal de flujo malintencionadamente pudiera obtenerlos.

Otro servicio de suma importancia es la gestión de bases de datos. Desde hace ya muchos años se viene haciendo uso extendido de los sistemas de gestión de bases de datos con cientos de propósitos, pero en los últimos años se han apoderado de casi la totalidad de la gestión en la web [55]. Son muchos los ejemplos de sistemas de bases de datos soportados sobre la web, dignos a destacar son los popularizados CMS, funcionales aplicaciones que han desarrollado la gestión de contenido y de información en general en el entorno de la web. Antaño conectar un sitio web a una base de datos solía ser tarea difícil, sobretodo en los sistemas de software libre, pues no disponían de soporte para interfaces estandarizadas como la Open Database Connectivity (ODBC). Hoy día esto ha cambiado y proyectos muy serios han llenado esta carencia en el campo del software libre.

### 3.3.2.3.1. Instalación y configuración del servidor Web.

El servidor HTTP Apache, es un software libre y de código abierto para las plataformas Windows, Mac OS X y UNIX (GNU, BSD, etc), en la cual se hace realidad y se implementa el protocolo HTTP 1.1 (Hypertext Transfer Protocol) y la noción de sitios virtuales. La instalación de Apache por lo general se combina con lenguajes de programación que soportan las prestaciones de la web dinámica, o sea, permiten el procesamiento en el lado del servidor. Algunas muy comunes en el software libre son Ruby, Python, Java y PHP (Preprocesador de Hipertexto), a esta última le dedicamos una sección a continuación, pues es el que más popularidad ha alcanzado en los últimos tiempos en conjunción con servidores de bases de datos relacionados como MySQL (del que se habla en próximos subepígrafes), para la confección de aplicaciones web dinámicas.

La tarea de instalación de Apache en FreeBSD se simplifica en gran medida utilizando la colección de Port, en la que podemos encontrar diferentes versiones del servidor Apache, por un lado tenemos la 1.3 una rama de elevada madurez en el código y muchos años de depuración y prueba, por el otro tenemos las distintas versiones 2.X que son mucho más modernas y su desarrollo más activo, esta rama es una completa reescritura del código y añade nuevas características como la interacción con el kernel en el procesamiento multitarea y una arquitectura altamente modular que trae considerables beneficios en el momento de configurar y ajustar el rendimiento. Este trabajo refiere a la versión 2.2.

#### Instalación de PHP.

Para instalar PHP [G] en el sistema, se puede hacer uso del árbol de Ports de FreeBSD:

```
# cd /usr/ports/lang/php5  
# make config ; make install
```

Aparece un menú, donde se debe marcar Apache para la instalación del módulo correspondiente. El resto de las opciones permanecerán tal cual. La configuración de PHP descansa en el fichero */usr/local/etc/php.ini*, para habilitarlo sería:

```
# cd /usr/local/etc  
# cp php.ini-recommended php.ini
```

Ahora se puede proceder con la instalación de Apache [G]. La instalación de Apache utilizando los Ports puede hacerse utilizando los comandos siguientes:

```
# cd /usr/ports/www/apache22  
# make config ; make install
```

Deberá aparecer un menú<sup>13</sup> con las opciones de instalación, entre las aparecen algunos de los módulos de Apache, se seleccionan las opciones necesarias y se procede con la instalación:

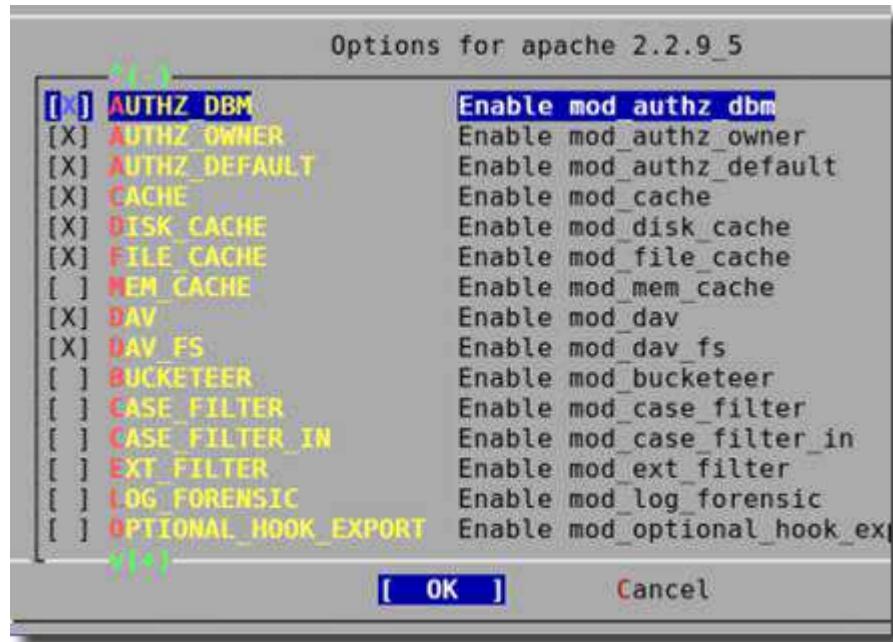


Fig. 3.4 Menú ncurses para configurar la instalación del Port de Apache.

Una vez que el proceso de instalación sea completado, se puede entonces personalizar la configuración de Apache, se debe tener en cuenta la integración con el módulo de PHP:

```
# cp /usr/local/etc/apache22/httpd.conf /root/httpd.conf.bak
# ee /usr/local/etc/apache22/httpd.conf
```

```
...
#ServerAdmin you@example.com
ServerAdmin webmaster@icm.cu
...
...
#ServerName host.example.com:80
ServerName www.icm.cu:80
...
...
<IfModule dir_module>
    DirectoryIndex index.php index.html
</IfModule>
...
...
AddType application/x-httpd-php .php
AddType application/x-httpd-php-source .phps
```

<sup>13</sup> Es frecuente configurar una instalación personalizada de los Ports, para personalizar la instalación se utiliza un menú ncurses (sistemas gráficos de consola de texto) donde se marcan las opciones de instalación deseadas. Si se desea reinstalar el Port con una nueva configuración, es necesario llamar al menú explícitamente mediante el comando "make config".

Es posible chequear la corrección del fichero de configuración una vez modificado, esto se puede hacer con el comando:

```
# apachectl configtest
```

En caso de que el fichero este correcto la salida del comando será **syntax ok**. En caso contrario la utilidad reportará el error y el número de línea donde se ubica.

En las versiones 2.X, la interacción con el kernel reporta un error, cuando se carga un módulo del kernel, en el instante en que inicia la máquina. Para corregirlo será necesario cargar este modulo en el arranque del sistema, esto sería:

```
# echo 'accf_http_load="YES"' >> /boot/loader.conf
```

Finalmente configurar el inicio del servicio en el fichero */etc/rc.conf*:

```
# echo 'apache22_enable="YES"' >> /etc/rc.conf
# echo 'apache22_http_accept_enable="YES"' >> /etc/rc.conf
```

Ahora todo está listo para arrancar el servicio (será sugerente reiniciar la máquina o cargar el módulo del kernel manualmente) con el comando:

```
# /usr/local/etc/rc.d/apache22 start
```

Podemos entonces verificar el funcionamiento correcto del servidor utilizando un navegador (existen algunos de interfaz de consola de texto como el Lynx) o con el comando:

```
# telnet localhost 80
```

Que nos debe dar una salida semejante a esta:

```
Trying 127.0.0.1...
Connected to localhost.
Escape character is '^]'.

GET / HTTP/1.0
HTTP/1.1 200 OK
Date: Sat, 01 Mar 2008 02:00:30 GMT
Server: Apache/2.2.8 (FreeBSD) mod_ssl/2.2.8 OpenSSL/0.9.8g DAV/2
Last-Modified: Sat, 20 Nov 2004 20:16:24 GMT
ETag: "cf597-2c-4c23b600"
Accept-Ranges: bytes
Content-Length: 44
Connection: close
Content-Type: text/html
<html><body><h1>It works!</h1></body></html>
Connection closed by foreign host.
```

Es válido destacar el carácter modular de Apache (sobretodo las últimas versiones). Decenas de módulos se tienen a disposición que aportan al complemento y la expansión funcional de este servidor. A continuación se muestra una lista de los módulos más populares, en la Internet se pueden encontrar muchos más:

- *mod\_ssl*: Brindando comunicaciones seguras vía SSL (Secure Sockets Layer) y TLS (Transport Layer Security).
- *mod\_rewrite*: Conocido también como reescritura de direcciones o URL, sirven para reescribir URL dinámicas y transformarlas en estáticas.
- *mod\_dav*: Con soporte para el protocolo WebDav.
- *mod\_auth\_ldap*: Permitiendo autenticar usuarios con la ayuda de LDAP (Lightweight Directory Access Protocol).
- *mod\_security*: Gestiona aspectos avanzados de la seguridad del servidor y del protocolo HTTP.
- *mod\_evasive*: Protege el servidor Apache contra ataques de DOS.
- *mod\_perl*: Soporte para el lenguaje de programación Perl.
- *mod\_php* : Soporte para el lenguaje de programación PHP.
- *mod\_python*: Soporte para los sitios dinámicos realizados en Python.
- *mod\_ruby*: Soporte para el lenguaje de programación Ruby.
- *mod\_mono*: Soporte para el proyecto MONO, la implementación .NET en GNU/Linux.

### 3.3.2.3.2. Instalación y configuración del servidor FTP.

En la colección de Port de FreeBSD contamos con una diversidad de prestigiosos servidores de FTP. Entre los más populares tenemos el WU-FTPD de la Universidad de Washington, el vsftpd servidor enfocado en la seguridad y usado en muchas distribuciones GNU/Linux, el ProFTPD con muchas facilidades para la configuración, entre otros.

Con vistas a facilitar el proceso de configuración compatibilizándolo con el proceso de configuración del servidor Apache y sin perder de vista la necesidad de buenos mecanismos de seguridad se ha escogido el ProFTPD para esta presentación. ProFTPD [56] fue desarrollado con el objetivo de crear un servidor FTP que pudiera ser administrado desde la configuración, la que posee una sintaxis similar a la de Apache. Este posee una configuración en bloques jerárquicos semejante a la que podemos apreciar en el fichero httpd.conf de Apache. Esto da como resultado un servidor con buenas prestaciones de restricciones de acceso y un alto nivel de configurabilidad. Es muy sugerente en servidores de hosting donde el administrador debe gestionar el Servidor Web y el Servidor FTP. Otra de las ventajas de este servidor es que, a diferencia de muchos otros, puede ejecutarse en modo independiente sin necesidad de atarlo al funcionamiento de superdemonio inetd.

Instalar ProFTP desde los Ports, sería:

```
# cd /usr/ports/ftp/proftpd  
# make config ; make install
```

Se pueden dejar las opciones de instalación que vienen por defecto o marcar los módulos que sean necesarios.

Se asume que serán usadas las carpetas por defecto de cada usuario */home/user* (por diferentes cuestiones entre ellas de seguridad, las carpetas bajo el */home* suelen separarse en una partición de disco aislada).

La configuración se realiza editando el fichero *proftpd.conf*, quedaría algo así:

```
# ee /usr/local/etc/proftpd.conf
```

```
...
ServerName "Servidor ProFTP en ICM"
ServerType standalone
...
...
DefaultServer on
...
...
AllowOverwrite on
...
...
AccessGrantMsg "Bienvenido a ICM"
AccessDenyMsg "Acceso Denegado"
...
...
AuthUserFile "/etc/passwd"
AuthGroupFile "/etc/group"
```

De esta forma se permite a los usuarios de sistemas acceder por FTP a sus carpetas bajo */home*, es importante hacer notar que no se ha habilitado el acceso anónimo (hacerlo resulta sencillo). Después de salvar la configuración y el ProFTPD quedará listo para iniciar, sólo restaría añadirlo al inicio del sistema en el fichero */etc/rc.conf*:

```
# echo 'proftpd_enable="YES"' >> /etc/rc.conf
```

Luego iniciar el servicio sería:

```
# /usr/local/etc/rc.d/proftpd start
```

### 3.3.2.3.3. Instalación del servidor de Bases de Datos.

En los sistemas FreeBSD no están disponibles de forma nativa los SGBD dominantes del mercado, como Oracle, MS-SQL y IBM DB2, ni algunos de los lenguajes de gestión dinámica en la web basados en Windows como ASP y ColdFusion. La tarea de la gestión de bases de datos en FreeBSD es llevada en gran medida por alternativas libres de SGML como MySQL y PostgreSQL y otros sistemas del mismo estilo, que combinados con lenguajes libres como PHP, Perl y Python nos brindan las herramientas necesarias para la elaboración de sistemas de gestión dinámica de web con respaldo de datos almacenados.

En los últimos tiempos el campo del software libre relacionado con la gestión de bases de datos está en constante crecimiento y a diario se desarrollan soluciones de gran utilidad. A los administradores de sistemas se les ha facilitado mucho la tarea de la selección de software con buen soporte de prestaciones, y esto es debido al gran impulso que han dado a esta rama los sistemas MySQL y PostgreSQL, quienes han entrado, incluso, en competencia con los grandes exponentes del género. Bien dotados de funciones y con altos rendimientos estos sistemas se han convertido en alternativas a considerar en lo que refiere a soluciones de software libre y a pesar de que entre ellos existen algunas diferencias ambos son más que aceptados y respetados. Entre estos sistemas las diferencias son meramente filosóficas. Por un lado MySQL aboga por un enfoque dirigido fundamentalmente a niveles altos de rendimiento y confiabilidad, siendo mucho más lento en el soporte de nuevas funcionalidades pues su grupo de desarrollo de MySQL AB alega que suelen ser fuente de riesgo que pueden comprometer la estabilidad del sistema. En cambio la prioridad de PostgreSQL se enfoca más en la completitud del sistema, su desarrollo se orienta en la mayor implementación posible de funcionalidades y flexibilidad. La finalidad de este último consiste en crear un reemplazo equivalente para los reconocidos líderes comerciales, dígase MS-SQL y Oracle. Cuando MySQL añade una nueva característica es altamente probable que esta ya esté implementada en PostgreSQL, pues se desarrolla más lentamente producto de que en la opinión de sus desarrolladores estas características son secundarias ante la garantía máxima de estabilidad y rendimiento.

Sin embargo MySQL es el sistema libre en este terreno más aceptado a nivel mundial. Estimaciones de Julio del 2004 mostrados en la revista SD Times, reportaban cerca de 11 millones de instalaciones, que representaba el 33% del mercado en el que competían los gigantes Oracle y Microsoft's SQL Server. Sin duda alguna MySQL ha sido el sistema libre escogido para este proyecto. Antes solamente señalar que en FreeBSD es posible instalar de forma no nativa (compatibilidad con Linux) sistemas como Oracle [57], y de igual modo se exhorta a que sea también probado el PostgreSQL como alternativa en los sistemas libres.

Instalar (Ports) MySQL en FreeBSD [G] sería:

```
# cd /usr/ports/databases/mysql50-server  
# make -D BUILD_OPTIMIZED install
```

Una vez que el proceso de instalación ha finalizado se puede configurar el sistema para su ejecución, se han dispuesto un conjunto de paso para organizar el proceso:

1.Ejecutar el script *mysql\_install\_db* para instalar las bases de datos del sistema, quedaría:

```
# mysql_install_db --user=mysql
```

2.Se inicia el servicio en modo seguro y se introduce la contraseña del administrador de MySQL (es posible usar este procedimiento si en algún momento se extravía la contraseña de administración del sistema):

```
# mysqld_safe &
# mysqladmin -u root password 'local'
# mysqladmin -u root -h host.example.com password 'remote'
```

3.Modificamos el fichero */etc/rc.conf* insertando la línea correspondiente a servidor MySQL:

```
# echo 'mysql_enable="YES"' >> /etc/rc.conf
```

4.Finalmente se debe reiniciar el servicio para que salga del modo seguro:

```
# /usr/local/etc/rc.d/mysql-server restart
```

Para verificar su funcionamiento correcto se puede utilizar el comando:

```
# mysqlshow -p
```

Este comando mostrará las bases de datos del sistema. La salida de este comando quedaría:

Databases	
information_schema	
mysql	
test	

### 3.3.2.4. Servidor de correo corporativo.

No se concibe, en los últimos tiempos una red corporativa que no ofrezca servicios de correo electrónico a sus usuarios. Muchas sociedades han ganado en cultura de intercambio de correo electrónico, llegando a complementar otros medios de comunicación y difusión como la correspondencia postal, el teléfono, la radio y la televisión. En esto ha tenido gran influencia la prestación de servicios públicos gratuitos muy populares en la Internet de acceso a este recurso como Yahoo, Gmail, etc. Pero como es lógico, a la gran mayoría de los usuarios finales esto representa una caja negra, de modo que operan exentos del respaldo tecnológico y de la infraestructura que mantiene funcionando tan eficientemente este servicio. Pero, mantener un servicio de correos en los últimos tiempos no es tan sencillo como solía serlo en sus inicios. Con la proliferación por este medio de virus, gusanos, troyanos, spam y todo esto sin mencionar que los usuarios esperan un servicio ininterrumpido (semejante a como lo hace el teléfono), la prestación de estos servicios se ha convertido en un ardua tarea. Además, aparecen nuevas tecnologías referentes a seguridad y requerimientos nuevas prestaciones en la protección de contenido solicitadas por productos comerciales.

En cada servidor de correo se ejecuta un MTA (Mail Transfer Agent), sistema que juega el rol primario en el intercambio de correo electrónico, pues se encarga de establecer sesiones de transferencia con MTAs de otros servidores mediante el protocolo simple de transferencia de correo SMTP.

La primera tarea, antes de comenzar con la instalación de un MTA es verificar que está correctamente configurado el registro "MX" en nuestro DNS, es también muy recomendable tener configurada la resolución inversa (rDNS), pues algunos servidores la chequean como mecanismo de autenticidad, recordemos que esta es la forma en que los servidores externos serán capaces de reconocer cual es el servidor de correo de cada dominio. Un servidor remoto entregará el correo al servidor identificado en el registro "MX" de menor prioridad, si no es alcanzable continuar con el siguiente y así sucesivamente hasta establecer la sesión o dar los correos por no entregados, los cuales van entonces a una cola de reintento.

Cuando un usuario se conecta, bien sea local o remotamente, lo hace mediante un MUA (Mail Transfer Agent), conocidos también como programas clientes de correo. En la recepción de mensajes, cada MTA almacena los correos en carpetas (buzón de destinatario), donde son accedidos luego por los MUA que permiten leerlos localmente (si está en el mismo servidor) o remotamente mediante el uso de los protocolos POP o IMAP. El envío por parte de los MUA, se realiza entregando al servidor los mensajes utilizando el protocolo SMTP. Los mensajes son depositados en una cola de procesamiento, hasta que el servidor termine las sesiones de recepción y esté listo para ejecutar el envío (en muchos servidores esto ocurre simultáneamente). Todo este proceso es conocido como *relay*, y no sólo ocurre con clientes, es posible configurarlo para permitir el acceso de otros servidores (smarthost) a esta prestación. La configuración de este mecanismo se debe hacer con mucha precaución, pues se corre el riesgo de dejar una brecha abierta que puede ser usada malintencionadamente, donde se puede aprovechar la apertura de la posibilidad de relay (open relay) para distribuir mensajes con contenidos basura. Los servidores de relay abierto son muy censurados en la Internet, pues además de la divulgación de correos no deseados, congestionan las redes con volúmenes de tráfico innecesarios.

### 3.3.2.4.1. Selección de un MTA libre.

En FreeBSD se cuenta con toda una variedad de MTA libres que van desde el antológico *Sendmail* (viene instalado por defecto en el sistema base) hasta otros más modernos y ágiles como *Exim*, *Qmail*, *Postfix*, *Courrier MTA* y otros tantos.

La selección debe estar enfocada fundamentalmente a la agilidad, versatilidad y flexibilidad, por lo que de esta lista se le ha dado el voto de confianza a **Exim** (EXperimental Internet Mailer), un MTA desarrollado por la Universidad de Cambridge y puede ser utilizado en la mayoría de los sistemas UNIX-like, si bien puede compilarse en sistemas operativos Windows, no se recomiendan estos sistemas como plataforma adecuada para utilizarlo como servidor de producción. Es un MTA monolítico y ligero, diseñado para servir de reemplazo por líneas de comando a sendmail (compatible con mailwrapper<sup>14</sup>). Se distribuye sin costo bajo la licencia GNU/GPL por lo que es, además, software libre. El proyecto cuenta con buena documentación [58], ejemplos y recetas claras de “como hacer” determinadas tareas.

En términos generales se destaca que no existen situaciones para las que Exim sea una opción incorrecta y en muchos casos se desempeña como la mejor opción. El desconocimiento y la no selección de este MTA van ligado fundamentalmente a razones subjetivas, pues la semántica de la configuración difiere (por lo que dificulta su comprensión) de otros populares MTA como *Sendmail* (el más frecuente en literatura del tema) y *Postfix* (sencillo de configurar y mantener). Como punto a favor de Exim está el hecho de que es el MTA por defecto en las distribuciones Debian GNU/Linux. A continuación se listan las principales características:

- La gran flexibilidad en los caminos que pueden seguir los mensajes según su origen.
- Buenos mecanismos de reintento (requeueing), mediante poderosos algoritmos.
- Compatibilidad con sistemas de control de spam, virus y listas negras (DNSBL).
- Control de relay mediante listas de acceso y mecanismos de autenticación.
- Integración con sistemas de directorios y bases de datos para la gestión de usuarios y dominios virtuales.
- Integración sencilla con los clientes SMTP o los clientes y servidores POP y IMAP.

<sup>14</sup> *mailwrapper* representa una capa de abstracción que permite reemplazar fácil y transparentemente sendmail por otro MTA sin intervenir en modo de funcionamiento del sistema. El comando `/usr/sbin/sendmail` es un enlace duro al `/usr/sbin/mailwrapper`, quien a su vez utiliza el fichero `/etc/mail/mailert.conf` para ejecutar redirecciones de comandos (llamadas a sendmail).

### 3.3.2.4.2. Sistema de administración de dominios virtuales.

La solución propuesta se basa en la implementación del un sistema integrado conocido como VExim, un sistema basado en PHP y MySQL ideado para el manejo de múltiples dominios y usuarios virtuales, de este modo Exim es usado para recepcionar el correo de los usuarios y mediante la utilización de bases de datos, se almacenan los datos de los usuarios como las contraseñas y el resto de la información de configuración de cuentas.

Local domains	Admin account	Total admins
alien8.co.uk	[REDACTED]@alien8.co.uk	1
asylum-net.org	[REDACTED]@asylum-net.org	2
asylumnet.org	[REDACTED]@asylumnet.org	2
edgington.org	[REDACTED]@edgington.org	1
mountaingrill.co.uk	[REDACTED]@mountaingrill.co.uk	1
silverwraith.com	[REDACTED]@silverwraith.com	1

**WARNING:** Deleting a domain will delete all user accounts in that domain permanently!

**Relay domains**

- copsys.co.uk
- exile.asylumnet.org
- legolas.com

**Aliased domains**

- avleen.com -> silverwraith.com

Fig. 3.5 Panel de administración web de VExim.

VExim integra la mayor parte de las posibilidades de Exim en una configuración sólida y organizada, integrada con sistemas externos, que colaboran en el manejo de las diferentes funcionalidades. Además nos ofrece una trabajada interfaz de administración mediante la web, un panel de control donde podemos administrar todo el sistema de una forma más asequible. Esta instalación convierte un conjunto de herramientas aisladas en una completa solución de correo electrónico. Se trabaja con la versión 2 donde las principales características son:

- Seguridad.
  - Antispam y Antivirus
  - Autenticación de usuarios.
  - Mecanismos autenticados de relay.
  - Entorno protegido de administración.

- Integración de software.
  - Antispam, SpamAssassin.
  - Antivirus, Cualquier escáner de virus compatible con Exim
  - Entrega, Procmail u otro software al que los correos puedan ser redirigidos.
  - Respaldo en bases de datos de MySQL o PostgreSQL utilizando PearDB.
  - Traducciones a diferentes idiomas.
- Panel de control Web.
  - Manejo de dominios locales virtuales y relay virtuales de forma sencilla
  - Tratamiento de alias de dominio.
  - Manejo de cuotas por dominio
  - Posibilidad de seleccionar UIG/GID del sistema o virtual para cada dominio.
  - Limites en la cantidad de cuentas por dominio
  - Menús ordenados y lista de dominios.
- Administración de dominios.
  - Fácil creación de cuentas de correo o alias accesibles vía POP/IMAP.
  - Habilitar o deshabilitar cuentas con facilidad.
  - Mecanismo de "catchall" para recoger los correos de dominios desconocidos.
  - Creación de entradas (:fail:) para forzar la redirección de correo a una dirección particular.
  - Cuotas opcionales en los buzones.
  - Delegar la administración de dominios.
  - Menús y listados alfabéticos de cuentas.
- Administración de cuentas.
  - Los usuarios pueden cambiar sus contraseñas
  - Es posible permitir a los usuarios ajustar la recepción de spams y virus en sus cuentas.
  - Es posible permitir a los usuarios ajustar las cuotas de su cuenta.
- Filtrado de mensajes.
  - Desde el panel de control se habilita el sistema antispam para cada dominio.
  - Es posible permitir a los usuarios ajustar la recepción de spams y virus en sus cuentas.
  - Permite a los usuarios configurar mensajes de “vacaciones” para cuando no están revisando sus buzones.
  - Es posible reenviar (forward) todo el correo recibido por una cuenta a otra cuenta, habilitando una regla.

A continuación se muestra una guía para implantar este sistema en un servidor de producción:

### Instalación y configuración del Antivirus ClamAV.

ClamAV es un sistema antivirus conformado por los demonios clamd (atiende las solicitudes de chequeo) y freshclam (mantiene las bases actualizadas), y un conjunto de clientes que se ejecutan desde la línea de comando para efectuar diferentes tipos de análisis en búsqueda de virus. Una vez configurado Exim enviará las solicitudes al servidor clamd, y si un mensaje es clasificado como posible portador de un virus es rechazado y puesto en cuarentena por el Exim. ClamAV se puede instalar desde el árbol de Port:

```
# cd /usr/ports/security/clamav  
# make install
```

Su inicio con el arranque del sistema se configura en el fichero */etc/rc.conf*:

```
# echo 'clamav_clamd_enable="YES"' >> /etc/rc.conf  
# echo 'clamav_freshclam_enable="YES"' >> /etc/rc.conf
```

La configuración se realiza editando el fichero */usr/local/etc/clamd.conf* donde se cambian algunos parámetros, el resto continúa con los valores por defecto:

```
# ee /usr/local/etc/clamd.conf
```

```
...  
LogFile /var/log/clamav/clamd.log  
...  
...  
PidFile /var/run/clamav/clamd.pid  
...  
...  
LocalSocket /var/run/clamav/clamd  
...  
...  
DatabaseDirectory /var/db/clamav  
...
```

Luego se configura el servicio (demonio) de actualización */usr/local/etc/freshclam.conf*:

```
# ee /usr/local/etc/freshclam.conf
```

```
...  
DatabaseDirectory /var/db/clamav  
...  
UpdateLogFile /var/log/clamav/freshclam.log  
...  
PidFile /var/run/clamav/freshclam.pid  
...  
DatabaseMirror database.clamav.net
```

Iniciar los servicios clamd y freshclam:

```
# /usr/local/etc/rc.d/clamav-clamd start  
# /usr/local/etc/rc.d/clamav-freshclam start
```

De esta forma queda el sistema antivirus instalado configurado y andando, listo para ser integrado con otros sistemas de donde provienen las solicitudes. La actualización es automática, pero no está de más chequear el log de actualización.

### Instalación del antispam SpamAssassin.

SpamAssassin (SA) es una de las soluciones más acertadas para la lucha contra el spam, sobretodo en el campo del software libre. SA puede ejecutarse como un demonio (spamd) aceptando solicitudes provenientes de MTA o clientes de correo, para chequear cuando un correo debe ser clasificado como spam. El sistema analiza el correo acorde con un conjunto de parámetros y asigna un indicador de probabilidad de que el mensaje sea spam teniendo en cuenta el contenido analizado. Este indicador es devuelto al emisor de la solicitud, quien es el encargado de tomar decisiones (aceptar, rechazar o enviar a cuarentena) respecto al mensaje.

Instalar SA mediante los Ports:

```
# cd /usr/ports/mail/p5-Mail-SpamAssassin/  
# make config ; make install
```

Para configurar SA se editan los ficheros de configuración localizados en la carpeta */usr/local/etc/mail/spamassassin*. El proceso de compilación crea ficheros de ejemplo que deben ser modificados a las necesidades:

```
# cd /usr/local/etc/mail/spamassassin  
# cp local.cf.sample local.cf  
# ee local.cf
```

```
...  
trusted_networks 192.168.  
...  
...  
lock_method flock  
...  
...  
bayes_ignore_header X-Bogosity  
bayes_ignore_header X-Spam-Flag  
bayes_ignore_header X-Spam-Status  
...
```

Esto es básicamente el proceso de configuración, sólo resta obtener la última versión de las reglas y compilarlas, pues compiladas aumentan el rendimiento de sistema:

```
# sa-update -nogpg -D --channel updates.spamassassin.org
...
# sa-compile
...
```

Listo el sistema para arrancar, antes añadir la línea correspondiente al *rc.conf*:

```
# echo 'spamd_enable="YES"' >> /etc/rc.conf
```

E iniciar:

```
# /usr/local/etc/rc.d/sa-spamd start
```

### **Instalación VExim.**

El paquete de instalación de VExim viene acompañado de dos ficheros de recomendada lectura antes de la instalación el *README.txt* y el *INSTALL.txt*, este último brinda una descripción del proceso de instalación paso a paso de VExim así como de sus componentes. Es muy recomendable un conjunto de conocimientos básicos de Exim y MySQL. Para comenzar con la instalación se seguirán los pasos del *INSTALL.txt*:

Se asume que ya no será necesario descargar el paquete de instalación, por lo que el próximo paso seria la creación de VirtualHost en Apache donde vamos a alojar el panel de control de VExim, la carpeta seleccionada será */usr/local/vexim/* y será aquí donde se descomprime el contenido del paquete *vexim2.tar.gz*:

```
$ cp /usr/local/vexim
$ sudo tar zxvf /PATH/TO/vexim2.tar.gz
```

Se edita el fichero de configuración de VirtualHots de Apache:

```
# ee /usr/local/apache22/httpd-vhosts.conf
```

```
#####
#      VEXIM CONFIGURATOR
#####
<VirtualHost *:80>
    ServerAdmin postmaster@icm.cu
    ServerName cpvexim.icm.cu
    ServerAlias cpvexim.icm.cu
    DocumentRoot /usr/local/vexim
    <Directory /usr/local/vexim>
        Order Allow,Deny
        Allow from 200.55.136.168/48
    </Directory>
</VirtualHost>
```

En este instante el panel de control debe ser accesible desde la web, de modo que teniendo configurado el DNS con la dirección del VirtualHost de VExim se puede acceder al panel de control web de VExim desde la URL <http://cpvexim.icm.cu>.

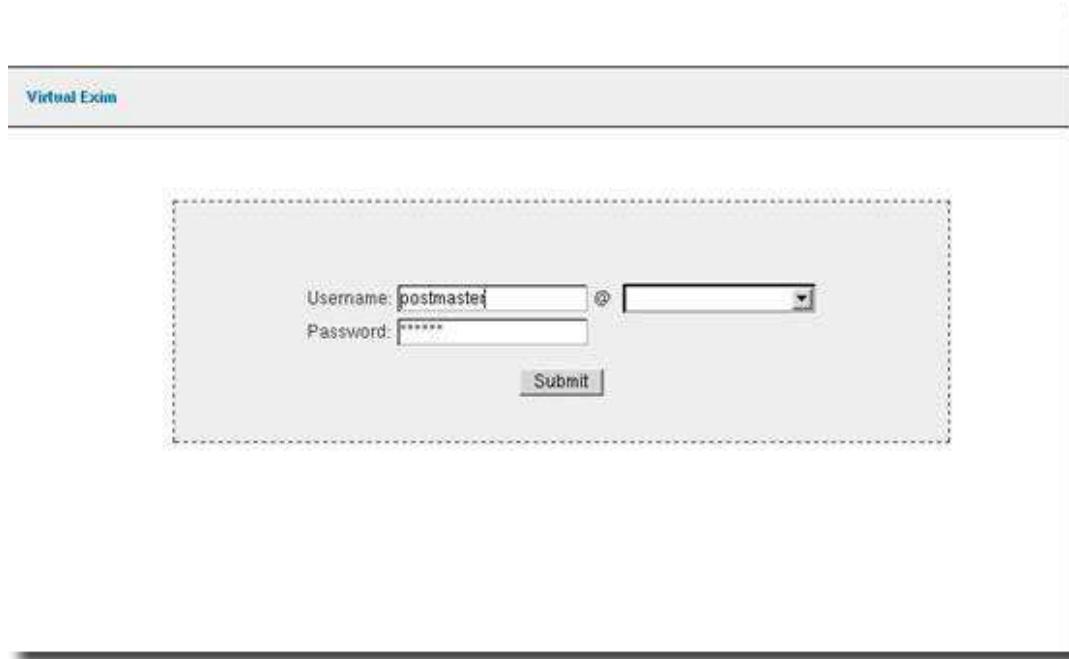


Fig. 3.6 Formulario de autenticación de VExim.

Para poder desde aquí realizar la configuración de la plataforma de servicios de correo en implantación será necesario antes crear la base de datos y el usuario con acceso. Es sugerente que se instale un servidor local (visto en epígrafes anteriores) por cuestiones de disponibilidad y seguridad (un servidor externo en este caso sería útil para mantener una replica de respaldo). VExim viene preparado para utilizar cualquiera de los servidores libres MySQL o PostgreSQL, en esta demostración se utiliza (por uniformidad) MySQL.

Para instalar la base de datos primeramente es necesario hacer algunas modificaciones necesarias en el script de creación *vexim2/setup/mysql.sql*, sustituyendo la palabra *CHANGE* por el dato que corresponda. En las líneas 6 y 7 se sustituye por *90* que será el UID/GID del usuario "*vexim*", luego en la línea 69 se reemplaza *CHANGE* por la contraseña (*veximICM2008*). Finalmente, el último de los *CHANGE* se puede dejar para ser modificado desde el panel de control web del sistema (pues se corresponde con la contraseña encriptada que viene en la plantilla de creación).

Una vez modificado el script se crea la base de datos ejecutando el comando:

```
# mysql -u root -p < vexim2/setup/mysql.sql
```

Finalmente, para acceder desde el panel de control web se modifica el fichero *vexim2/vexim/config/variables.php*, asignando los valores correspondientes a las variables. Luego el panel de control está listo para administrar el sistema VExim.

## Instalación Exim y configuración integrada con VExim.

Según se menciona anteriormente, procede antes de instalar el servidor Exim chequear el correcto funcionamiento de nuestro DNS, para esto se puede hacer uso del comando *dig*, este comando solo funciona en sistemas operativos de tipo UNIX-like (en otros sistemas operativos se puede utilizar el *nslookup*):

```
# dig @ns1.icm.cu icm.cu mx
```

En las últimas versiones de FreeBSD, se ha simplificado instalar Exim desde los Ports, incluso en ajuste con los caso de uso el equipo de desarrollo han creado Ports personalizados, para distintos tipos de instalaciones de Exim (independientemente de que las instalaciones de los Ports se pueden ajustar mediante parámetros). La que se ajusta con los requerimientos es la de *exim-mysql* que soporta la integración de servidor Exim con el respaldo de bases de datos en MySQL. El procedimiento de instalación sería:

```
# cd /usr/ports/mail/exim-mysql/
# make install
```

Una vez instalado, el paso siguiente será configurar el *mailwrapper*, para sustituir *sendmail*, en MTA instalado por defecto en el sistema base. Antes de efectuar esta operación es necesario detener el demonio de *sendmail*:

```
# /etc/rc.d/sendmail stop
```

Configurar<sup>15</sup> el *rc.conf*:

```
# echo 'sendmail_enable="YES"' >> /etc/rc.conf
# echo 'sendmail_flags="-bd -q15m"' >> /etc/rc.conf
# echo 'sendmail_submit_enable="NO"' >> /etc/rc.conf
# echo 'sendmail_outbound_enable="NO"' >> /etc/rc.conf
# echo 'sendmail_msp_queue_enable="NO"' >> /etc/rc.conf
```

Configurar el *mailer.conf*:

```
# ee /etc/mail/mailer.conf
```

sendmail	/usr/local/sbin/exim
send-mail	/usr/local/sbin/exim
mailq	/usr/local/sbin/exim -bp
newaliases	/usr/local/sbin/exim
hoststat	/usr/local/sbin/exim
purgestat	/usr/local/sbin/exim

<sup>15</sup> Es posible remplazar *sendmail\_enable="YES"* por *exim\_enable="YES"*, pero de la forma utilizada se aprovecha el script de inicio */etc/rc.d/sendmail* para operar con el demonio del servidor Exim.

Una vez que se ha terminado de instalar Exim, el paso que sigue es la configuración, para ello es necesario sustituir el archivo de configuración original de Exim */usr/local/etc/exim/configure* por los que vienen en la distribución de VExim:

```
# mv /usr/local/etc/exim/configure /usr/local/etc/exim/configure.ORIG  
# cp -R vexim2/docs/* /usr/local/etc/exim/
```

Del mismo modo que el script de la bases de datos será necesario hacer ajustes en la configuración sustituyendo la palabra *CHANGE*. En la línea 78 se sustituye *CHANGE* por la contraseña del usuario "vexim".

A partir de la línea 268 comienzan las configuraciones de la listas de acceso, donde se recomienda deshabilitarlas (comentando o eliminando la línea), para luego haciendo pruebas habilitarlas una a una. La configuración de estas ACL incide directamente en la capacidad de recepción de mensajes en el servidor, por tal razón se recomienda proceder con cuidado. Las ACL interceptan los mensajes en un preprocesamiento, antes de ser aceptados por el servidor. En este caso tenemos los analizadores de spam y virus y las listas negras de bloqueo por DNS. Cada administrador es el encargado de decidir los niveles de bloqueo de su servidor.

Finalmente, se puede notar que gracias a la versatilidad del sistema con la configuración respaldada en una base de datos, los cambios en el fichero de configuración se minimizan, reduciendo de esta manera la introducción de errores. Organiza de forma limpia el proceso sin necesidad de la introducción de parches y soluciones puntuales.

### 3.3.2.4.3. Acceso de clientes, POP3, IMAP y corporativos.

Un proceso que va estrechamente ligado y la razón de ser de los servidores de correo es el acceso al correo por parte de los usuarios. Hasta este instante se había trabajado sobre el envío y la recepción de los mensajes en el servidor usando el protocolo SMTP. Lo que corresponde ahora será configurar los protocolos de cliente POP (Post Office Protocol) e IMAP (Internet Message Access Protocol), para que los usuarios puedan acceder a la lectura de sus correos. El protocolo POP permite a los usuarios descargar el correo hacia sus máquinas y el IMAP permite accederlo remotamente sin ser descargado, estos procesos son realizados por los MUAs, actualmente se cuenta con una buena variedad de aplicaciones clientes que van desde los que de usan en la consola (Ej *Pine* y *Mutt*) a los interactivos y gráficos clientes de escritor (Ej *Evolution* y *Mozilla Thunderbird*).

En el servidor se almacenan separadamente los correos de los usuarios, existen varios formatos de almacenamiento de los correos, los más conocidos son el fichero acumulativo *mailbox* y el uso de carpetas *maildir*. *mailbox* (mbox), mantiene todos los correos de un usuario en un mismo fichero, de modo que todas las operaciones se realizan con operaciones de lectura y escritura sobre el fichero, este formato es más antiguo, data de los tiempos en que el flujo de correos en la Internet no solía ser tan intenso. Por otro lado, *maildir* almacena de forma organizada los correos como ficheros independientes en la carpeta *maildir* (buzón de correo de usuario) este formato es más moderno y compatible más con el protocolo IMAP, pues recordemos que IMAP accede directamente a las carpetas en el servidor, fue introducido inicialmente por el servidor *Qmail*.

A diferencia del SMTP, los protocolos POP e IMAP requieren autenticación pues se preservan de forma separada los correos de cada usuario, es decir, un usuario necesita autentificarse en el servidor, y de esta forma podrá acceder única y exclusivamente a sus correos. Los sistemas que brindan servicios con estos protocolos son conocidos como servidores POP3 (version 3 del protocolo POP) e IMAP. Entre los más populares que están a disposición en FreeBSD están el *Qpopper* e *IMAP-UW* servidores de POP3 e IMAP respectivamente que se manejan desde el superdemonio *inetd*, además tenemos soluciones integradas (brindan ambos servicios) de servidores como el Cyrus-IMAP (autentica contra Cyrus-SASLAuth) y el Courier-IMAP (autentica contra Courier-authlib).

Es seleccionado en este proyecto es Courier-IMAP, un servidor IMAP libre que puede ser combinado con diferentes tipos de servidores MTA. Brinda acceso a las carpetas en formato *maildir*. Añadidamente viene con un servidor POP3 incorporado. Puede utilizar los mecanismos de autenticación que brinda Courier-authlib, que brinda servicios de autenticación con diversos soportes de respaldo, originalmente viene configurado para autenticar contra el fichero de usuarios del sistema */etc/master.passwd*, aunque puede ser configurado para autenticar contra bases de datos MySQL o PAM (esto incluye los modulos de PAM).

Para instalar este servidor es necesario primero instalar y configurar el demonio de autenticación Courier-authlib [59]. Se puede utilizar el árbol de Ports de la forma siguiente:

```
# cd /usr/ports/security/courier-authlib  
# make config ; make -DWITH_MYSQL install clean
```

En el menú que aparece se deben seleccionar los módulos de autenticación deseados, en el caso que ocupa se necesitará el módulo de autenticación contra bases de datos MySQL. Para la configuración de este demonio se debes modificar el fichero */usr/local/etc/authlib/authdaemonrc* donde se debe modificar la lista de módulos:

```
# ee /usr/local/etc/authlib/authdaemonrc
```

```
authmodulelistorig="authmysql"
```

Luego se configura el módulo en cuestión `/usr/local/etc/authlib/authmysqlrc`:

```
# ee /usr/local/etc/authlib/authmysqlrc
```

```
...
MYSQL_SERVER      localhost
MYSQL_USERNAME    vexim
MYSQL_PASSWORD    veximICM2008
...
...
MYSQL_DATABASE    vexim
MYSQL_USER_TABLE  users
MYSQL_CRYPT_PWFIELD crypt
...
MYSQL_UID_FIELD   uid
MYSQL_GID_FIELD   gid
MYSQL_LOGIN_FIELD id
MYSQL_HOME_FIELD  home
MYSQL_NAME_FIELD  name
...
```

Instalar (Ports) y configurar los servidores IMAP y POP3:

```
# cd /usr/ports/mail/courier-imap
# make config ; make install clean
```

En el menú aparece un conjunto de opciones para la instalación de Courier-IMAP [60], donde se pueden dejar las opciones por defecto. Para configurarlo podemos editar los archivos `/usr/local/etc/courier-imap/pop3d` y `/usr/local/etc/courier-imap/imapd` que son los ficheros de configuración de los servicios, además en esta carpeta tenemos los ficheros con nombre similar pero con sufijo "-ssl" que se utilizan para configurar las prestaciones bajo protocolos seguros de estos servicios.

Una vez que se ha configurado el Courier-authlib para autenticar estos servicios, no será necesario modificar la configuración salvo que deseemos personalizar alguna característica específica. Ahora todo está listo para arrancar los demonios correspondientes, para ello se utilizan los script de manipulación que provee el paquete de instalación y copiándolos a la carpeta `/usr/local/etc/rc.d` para que inicien con el arranque del sistema:

```
# cp /usr/lib/courier-imap/libexec/pop3d.rc /usr/local/etc/rc.d/
# cp /usr/lib/courier-imap/libexec/imapd.rc /usr/local/etc/rc.d/

# /usr/local/etc/rc.d/pop3d.sh start
# /usr/local/etc/rc.d/imapd.sh start
```

Otra cuestión es el acceso a buzones corporativos mediante multipop que se utiliza para gestionar y almacenar la totalidad del correo entrante de un dominio dado, de modo que el "servidor" de ese dominio, no recepciona sus correos de la forma convencional (por SMTP), sino que utiliza el protocolo POP3.

Para realizar esta tarea un MTA se configura de modo tal que para estos dominios especificados todo el correo se almacena en un solo buzón, luego desde el servidor remoto se accede autenticando contra el usuario (real o virtual) propietario de la carpeta contenedora y se descarga todo el correo utilizando el protocolo de cliente, entonces es separado localmente por usuarios en sus respectivos buzones y de esta manera los usuarios de esos dominios acceden con aplicaciones clientes a su correo.



Fig. 3.7 Configuración de cuentas de correo en VExim.

Exim brinda soporte [61] a este tipo de utilidad, soporte que ha sido aprovechado por los desarrolladores de VExim para incorporarlo en su aplicación. En VExim esta característica responde al nombre de *Catchall*, esto es, en los dominios especificados se configura una cuenta *Catchall* que atrapa todo el correo de ese dominio, para que luego sea descargado por el servidor remoto mediante POP3 autenticando con los datos de la cuenta especificada.

#### 3.3.2.4.4. Acceso al correo desde la web.

Los administradores de servidores de correo, no deben, bajo ningún concepto, subestimar el nivel de confianza que depositan los usuarios en el correo electrónico. Se conocen muchos casos de empresas donde usuarios móviles redirigen su correo a servidores públicos (Ej. Yahoo, Hotmail, etc.) que ofrecen servicios de acceso web al correo (WebMail) cuando su empresa no brinda este tipo de servicio, este comportamiento es bien criticable, pero debemos tener en cuenta que los estándares de facto para el acceso remoto al correo, son sólo protocolos de comunicación que necesitan una aplicación capaz de gestionarlos, además no trafican libremente por la Internet. Es aquí donde entran en el juego los WebMail, una solución limpia, eficiente y segura. El uso de una WebMail simplifica la tarea de conseguir una aplicación cliente, pues utiliza el propio navegador como cliente, presente en la mayoría de los sistemas operativos gráficos. Con un cliente de correos basado en la web accesible en la Internet los usuarios pueden leer, enviar, recibir y organizar sus correos desde cualquier parte del mundo.

Existen connotados candidatos en el mundo del software libre, acá se propone uno de los más ligeros y populares de los clientes de correo web, además integrable en las plataformas de FreeBSD. El SquirrelMail [62a] una aplicación web de acceso al correo soportada sobre estándares y confeccionada con PHP. A pesar de ser un sistema ligero y fácil de instalar, es un proyecto [63b] serio y profesional. Es compatible con la mayoría de los navegadores web y provee las mismas funcionalidades básicas que las aplicaciones clientes de correo. Entre sus características más destacadas están:

- Soporte MIME para el manejo apropiado de adjuntos y correos multisección.
- Libreta de direcciones personal y manejo básico de contactos.
- Acceso y manejo a carpetas vía IMAP.
- Ajuste de preferencias y opciones relacionadas con la apariencia, leguajes y otros aspectos de interés al usuario.
- Extensibilidad mediante el uso de plugins para la incorporación de características no soportadas en el paquete original.

Una vez que están los prerequisitos instalados, el proceso de instalar SquirrelMail es muy simple:

```
# cd /usr/ports/mail/squirrelmail  
# make config ; make install
```

Para configurar SquirrelMail se pueden seguir los siguientes pasos:

1. Ajustar el fichero de configuración de PHP (*/usr/local/etc/php.ini*) si queremos incrementar el tamaño de los ficheros de subida, aunque el valor por defecto de 2MB es una buena medida.
2. Utilizar la herramienta de configuración de SquirrelMail e introducir los datos de la configuración:

```
# cd /usr/local/www/squirrelmail  
# ./configure
```

Es en una de las secciones que se indica que servidor IMAP se utiliza para acceder a las carpetas, en el caso que ocupa sería courier. Se debe tener en cuenta también la integración con múltiples dominios virtuales.

3. El paso que sigue es la publicación web, esto se puede hacer editando un fichero de configuración de SquirrelMail que se incluye luego en la configuración del servidor Apache. El paquete de SquirrelMail trae un fichero individual (no se integra en el httpd.conf) para facilitar la configuración:

```
# ee /usr/local/etc/apache22/Includes/squirrelmail.conf
```

```
Alias /squirrelmail "/usr/local/www/squirrelmail/"  
  
<Directory "/usr/local/www/squirrelmail/">  
Options None  
AllowOverride None  
Order allow,deny  
Allow from all  
</Directory>
```

De esta forma (después de reiniciar el servidor Apache) el WebMail debe quedar accesible desde un navegador usando la dirección <http://mail.icm.cu/Squirrelmail>. Claro, es posible también configurarle un VirtualHost con nombre de dominio, semejante al que se usa para VExim.



Fig. 3.8 Cliente de correo web SquirrelMail.

### 3.4. Migración de los servidores de la red interna.

#### Concepción de una intranet corporativa.

Tanto el término de **Intranet** [63] como el de **Intranet Corporativa** son conceptos incorporados y plenamente aceptados en el mundo de las tecnologías de la información. La concepción de **Intranet** fue introducida por Steven L. Telleen en el año 1998 y fue caracterizada por el conjunto de contenidos bien definidos que se manipulan dentro del entorno de una organización, inicialmente se refería al compartimiento y al acceso de contenidos independiente y opuestamente de la web (formada por contenidos libremente accesibles por cualquier público). Con la evolución del concepto de red y sus diferentes modalidades este término ha evolucionado también tomando un carácter un tanto más general (Ej Infomed, Rimed, etc), de modo que su concepción inicial quedó acompañada de un apellido **Intranet Corporativa**.

Se entiende por **Intranet corporativa** a aquella intranet o red privada perteneciente a una empresa o corporación. El principal motivo que está llevando cada vez más a un importante número de compañías a desarrollar su propia intranet es la adquisición de conciencia por parte de los directivos de la importancia que tiene la gestión del conocimiento en el ámbito empresarial. De entre los posibles beneficios que puede traer una intranet corporativa suelen destacar para las empresas el aprendizaje y la evaluación de los procesos productivos en lo referente a calidad, productividad, eficacia y costes.

Tiene como función principal proveer lógica de negocios para aplicaciones de captura, informes y consultas con el fin de facilitar la producción de dichos grupos de trabajo; es también un importante medio de difusión de información interna a nivel de grupo de trabajo. Las redes internas corporativas son potentes herramientas que permiten divulgar información de la compañía a los empleados con efectividad, consiguiendo que estos estén permanentemente informados con las últimas novedades y datos de la organización. Tienen gran valor como repositorio documental, convirtiéndose en un factor determinante para conseguir el objetivo de la oficina sin papeles. Añadiéndoles funcionalidades como un buen buscador y una organización adecuada, se puede conseguir una consulta rápida y eficaz por parte de los empleados de un volumen importante de documentación. Deberían cumplir unos requisitos de accesibilidad web permitiendo su uso a la mayor parte de las personas, independientemente de sus limitaciones físicas o las derivadas de su entorno.

## Intranet ICM.

En la concepción de una Intranet Corporativa del Instituto Cubano de la Música pueden intervenir varios elementos, entre los que se tienen previstos en una etapa inicial conforman:

- La conformación del dominio, pues esto le daría una carácter seguro y privado a la(s) red(es) interna(s).
- Disponer mecanismos que permitan, en primera instancia, la publicación de un sitio web interno que permita la organización y el acceso a los contenidos del Instituto; esto con carácter futuro, podría evolucionar hacia un servidor de aplicaciones, donde se podría ejecutar sistemas de cómputo (preferiblemente software libre) que gestionen el trabajo del centro (catálogos, etc.).
- Habilitación de un servidor proxy que permita la navegación interna a los usuarios, con distintos niveles de acceso.
- Habilitación de un servidor de salva y distribución compartida de contenidos (ficheros) que gestionaría por grupos empresariales la compartimiento de información y contenidos de diferentes índoles (en el caso del instituto es muy recomendado el almacenamiento de multimedia).

### 3.4.1. Administración de redes mediante dominios.

Áreas especialmente sensibles en la temática de migración al software libre son la gestión de redes mediante dominios de administración, la centralización de accesos, políticas de grupos y

seguridad en general. En muchas organizaciones la autenticación, autorización, y los modelos de acceso a recursos que se construyen sobre redes empresariales se relacionan estrechamente con la estructura organizativa y los procesos en la entidad. Implica un gran riesgo delegar estas responsabilidades tanto localmente a las máquinas como a los usuarios.

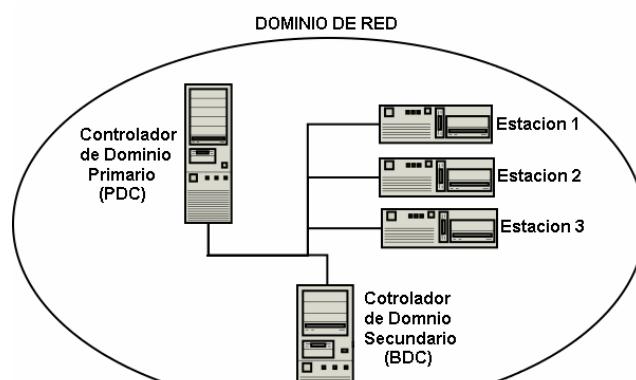


Fig. 3.9 Dominio de red con Controladores de Dominio.

Ciertamente, pasos agigantados se han dado y se continúan dando en la implementación de soluciones que representen alternativas a los estándares de facto que en este sector han impuesto las connnotadas soluciones de controladores de dominios de redes sobre las plataformas Windows® de Microsoft®. Definitivamente, es digno admitir que la primacía en estas tecnologías aún se conserva en manos del software privativo, y es por esta razón que la mayor parte de las soluciones que se conciben en el software libre no son más que acercamientos de imitación de su funcionamiento así como ajustes que permiten la coexistencia integrada de estos servicios en diferentes plataformas. De hecho son las soluciones mixtas las que actualmente están llamando más la atención, pues aunque no apuntan hacia una completa migración al software libre, juegan con las debilidades y capacidades de las diferentes plataformas, además sientan las bases en la

utilización de servidores UNIX-like en la gestión centralizada de dominios de redes, función que, aunque sus raíces datan de sus inicios [64], realmente no estaban del todo concebidas en la filosofía de estos sistemas, recordemos que, tanto el concepto de red empresarial como el de dominio de administración se han mantenido en constante evolución por lo que difieren mucho de sus inicios a la actualidad.

### **Controladores de Dominios con software libre.**

Actualmente, la mayor parte de los esfuerzos en la gestión de dominios de red con software libre están relacionados con Samba, un software que implementa de forma libre el protocolo de Servidor de Archivos SMB (Server Message Block) para los sistemas UNIX-like. De esta forma sistemas UNIX-like y Windows, pueden convivir bajo la misma arquitectura de red y con una perfecta comunicación e integración [65]. Para muchos usuarios, Samba es muchas cosas [66], pero en su concepción básica es un servidor de ficheros e impresión que se ha utilizado por mucho tiempo para emular productos de Microsoft®. Recientes investigaciones están utilizando Samba como plataforma incorporándole nuevos roles, entre ellos el de Controlador de Dominio (DC), donde combinado con los servicios de directorios LDAP, los más extendidos en el software libre (OpenLDAP), hace una perfecta compatibilidad con los sistemas de protocolos usados en los productos de Microsoft®, además Samba había sido dotado ya de mecanismos que le permiten a una estación de trabajo de plataforma UNIX-like integrarse a Directorios Activos en servidores Windows®.

Esta bivalencia está convirtiendo a Samba en el producto con más perspectivas en el desarrollo de tecnologías de interoperabilidad e integración de plataformas mixtas y redes. Muestra de ello son los esfuerzos que se llevan a cabo en la reescritura [J] del proyecto Samba en su versión 4 donde se persigue la meta de obtener una tecnología de DC totalmente compatible con el Directorio Activo y la posibilidad de que un cliente con Windows XP Professional pueda integrarse a este tipo de controlador de dominio del mismo modo que lo hace con un Directorio Activo, para esto el equipo de desarrollo de Samba4 ha decidido emular en lo mayor posible el modo de comunicación de los servidores de Windows 2003 Server, esto beneficia a otros desarrolladores de software que integran sus productos con dominios de Microsoft.

En la práctica, la implementación de soluciones en este sector del software libre es aún tema de estudio y experimentación, al punto de que hablar una solución concreta, que a su vez sea simple y transparente como las soluciones de Directorios Activos en los servidores Windows®, es prácticamente imposible, por esta razón en este epígrafe no se muestra una guía de implementación, sólo nos limitamos a brindar referencias para la investigación y profundización en el tema.

Es meritorio mencionar que algunas soluciones con distintos niveles de parcialidad se ponen a prueba con esperanzadores resultados y dan la medida de que no está lejano el día en que contemos con una alternativa sólida y consistente a las soluciones privativas.

Actualmente contamos con abundante documentación, reflejo del activo desarrollo, que aborda el tema de la integración de múltiples plataformas en dominios gestionados por controladores de dominios Samba. Algunos a modo general muestran la implementación de servidores Samba en

sistemas UNIX-like que operan como controladores de dominio [K][L] [67], otros particularizan esta tarea en distribuciones GNU/Linux como Debian [68a][68b] y CentOS [68c].

En cambio para nuestro protagonista FreeBSD y el resto de los BSDs, existe poca referencia, aunque esto realmente es relativo, pues existe una buena correspondencia y compatibilidad con la documentación citada en el párrafo anterior. Sólo han sido encontrados pocos manuales prácticos, uno de los más completos en alemán [69], otra buena referencia que servirá de punto de partida para proceder con esta tarea es la guía [70] que recientemente fue publicada en el sitio [www.bsdguides.org](http://www.bsdguides.org) donde Johan el autor nos muestra el proceso detallado para convertir un servidor FreeBSD en un Controlador de Dominio Primario utilizando la combinación Samba-OpenLDAP.

### 3.4.2. Gestión web de la Intranet.

Los entornos integrados de publicación web son paquetes de aplicaciones que traen soporte para la publicación de contenidos gestionados por aplicaciones web confeccionadas con software libre. Las más comunes están confeccionadas con PHP y con respaldo MySQL, entre la más populares y generales se encuentran los gestores de contenidos web (CMS). Estos entornos son conocidos como AMP [71], en un mismo paquete vienen el servidor web (generalmente Apache), los intérpretes PHP, Perl y otros (en ocasiones python), el servidor de bases de datos MySQL, y otras aplicaciones relacionadas como, phpMyAdmin.

Existen algunos de estos entornos para sistemas Windows (WAMP), uno muy recomendado es el UniformServer, existen algunos de estos paquetes para sistemas GNU/Linux (LAMP), pero en FreeBSD, lamentablemente, aún no se cuenta con uno de estos paquetes, en cambio Martin Munich nos ofrece una artículo [72] donde nos muestra la forma metodológica en que podemos emular un entorno LAMP en FreeBSD con todas las prestaciones.

#### 3.4.2.1. Gestores de Contenidos Web.

Los gestores de contenidos web han alcanzado funciones más allá de la confección de sitios web, que fue a grandes rasgos la idea inicial. Se han convertido en verdaderas aplicaciones de gestión organizativas, en varias ramas de las tecnologías de la información. Actualmente contamos con muchas aplicaciones de este tipo y las más renombradas por lo general estas confeccionadas bajo las normativas del software libre.

CMS son las siglas de Content Management System, que se traduce directamente al español como Sistema Gestor de Contenidos. Como su propio nombre indica, es un sistema que nos permite gestionar contenidos. En líneas generales, un CMS permitiría administrar contenidos en un medio digital y para el caso particular que nos ocupa, un CMS permitiría gestionar los contenidos de una web. Dicho de otra forma, un CMS es una herramienta que permite a un editor crear, clasificar y publicar cualquier tipo de información en una página web. Generalmente los CMS trabajan contra una base de datos, de modo que el editor simplemente actualiza una base de datos, incluyendo nueva información o editando la existente.

Un sitio de una intranet corporativa probablemente representará un sitio con elevado nivel de complejidad, pues en este quedará esquematizada en algún sentido la gestión de la empresa. Suele ser frecuentemente actualizado y las personas que editan la información no tienen rebuscados conocimientos de informática. A estos redactores se les tiene que facilitar el trabajo mediante una herramienta que les permita subir informaciones a la web y clasificarlas para que aparezcan en el lugar correcto. Por supuesto que estas personas no deben preocuparse con el código de la página ni las particularidades de programación de la plataforma donde esté alojada la web. Ellos sólo deben concentrarse en escribir las noticias, o cualquier tipo de contenidos y luego subirlas a la página por un sistema intuitivo y rápido. Una vez publicadas y clasificadas, las informaciones deben aparecer en la página web automáticamente, en los lugares donde haya decidido el editor.

Una herramienta CMS generalmente contendrá una interfaz basada en formularios, a los que habitualmente se accede con el navegador, donde se pueden dar de alta los contenidos fácilmente. Esos contenidos luego aparecerán en la página en los lugares donde se ha indicado al darlos de alta. Por lo tanto, un CMS estará compuesto de dos partes, un back y un front, siendo el back la parte donde los administradores publican las informaciones y el front la parte donde los visitantes visualizan las mismas.

### Ejemplos de CMS

A continuación se citan algunos ejemplos de CMS gratuitos y compatibles con algunos de los sistemas AMP a los que hacíamos referencia:

#### **Joomla!:** [73]

Es un CMS de código libre, considerado por muchos el mejor y con más facilidad de uso, está también creado en PHP. Surge como una mejora o ampliación de Mambo.

#### **Mambo:** [74]

Mambo es un sistema CMS libre y gratuito, creado en PHP.

#### **Drupal:** [75]

Uno de los CMS más populares, en este caso gratuito y open source. Creado en PHP y con posibilidad de utilizar varias bases de datos distintas, por defecto MySQL.

#### **Wordpress:** [76]

El CMS para la creación de blogs por excelencia, también creado en PHP y gratuito.

#### **OsCommerce:** [77]

El sistema gestor de contenidos de código libre, para la creación de una tienda más conocido y utilizado.

Esto es sólo una pequeña muestra pues el mundo de los CMS está ya bastante poblado. Solo nos resta sugerir el uso de un CMS para la confección de un sitio de intranet, pues sería una forma organizada y de fácil mantenimiento, además de que sería altamente compatible con las plataformas propuestas.

### 3.4.3. Servidor Proxy.

En las redes empresariales implica mucha utilidad la utilización de un servidor Proxy Web. Estos servidores frecuentemente se instalan en lugares intermedios donde los usuarios de la red pueden hacer uso del mismo sirviéndose de los servicios de la navegación web hacia el exterior. Los servidores proxies pueden llegar a ser bien complejos, los más simples son llamados pasarelas o túneles, algunos pueden modificar las solicitudes de los clientes o las respuestas de los servidores. Estos pueden servir en varias de las funciones, las más comunes son:

- **Proxy Cache:** Se utilizan para acelerar los servicios de navegación, pues mantienen almacenadas residentemente los contenidos de las respuestas que son frecuentemente solicitadas por los clientes. De esta forma cuando llega una nueva solicitud el Proxy responde con la que tiene en el cache sin salir a buscarla al servidor que la originó. Esto a su vez reduce en gran medida el uso de ancho de banda y con ello el costo y al mismo tiempo incrementa el rendimiento. Por su naturaleza fueron los primeros proxies concebidos.
- **Filtro de contenidos:** Este tipo de proxies brindan control administrativo sobre el contenido que circula por él. Es frecuente este tipo de Proxy en empresas comerciales y en escuelas, donde no todos los contenidos son permitidos a los usuarios. Los filtros son aplicados de varias formas, URLs y listas negras de DNS, incluso en algunos países se utilizan para restricciones de solo uso de navegación nacional. Suelen estar acompañados de mecanismos de autenticación que delimitan privilegios de acceso en los usuarios, acompañados de generación de logs y control de ancho de banda, además se integran con antivirus que protegen las redes internas de la entrada de contenido malicioso.
- **Interceptor:** También llamado "proxy transparente", es una combinación de los anteriores que emula los proxies de pasarela pues el acceso, cuando es permitido, queda transparente al usuario. De esta forma no es necesaria la configuración de aplicaciones clientes, son muy utilizados como mecanismos de protección, pues no compatibilizan con mecanismos de autenticación complejos.

### 3.4.3.1. Análisis de Hardware.

Con frecuencia los servidores Proxy son servidores de alto consumo, por lo que requieren un hardware apropiado. Sin embargo, en la selección de este servidor se han reducido los requerimientos con respecto a los servidores de producción de la DMZ, pues si bien no es aconsejable una PC de escritorio, tampoco se requiere un servidor demasiado potente, pues quedaría subutilizado. Para las prestaciones en las redes internas, es más que suficiente un buen servidor profesional de gama baja, con parámetros moderados de hardware.

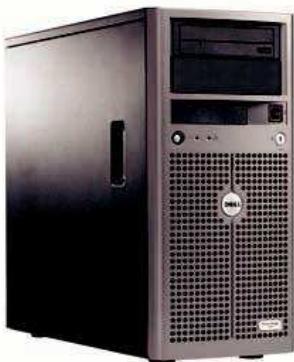


Fig. 3.10 Servidor gama baja Dell™ Poweredge™ 840.

Por tal motivo y teniendo presente el propósito de renovar la tecnología de los servidores de red, en la oferta que se comentó anteriormente, fueron incluidos también servidores adecuados para este tipo de prestaciones. Para la operación en las redes internas han sido considerado apropiado el servidor Dell™ Poweredge™ 840. En el **Anexo II.F** se puede apreciar la ficha técnica de estos equipos.

### 3.4.3.2. Instalación y configuración de un servidor proxy.

No cabe la menor duda de que al momento de hacer una selección de un proxy web libre, no hay mejor candidato que Squid. El proyecto Squid comenzó en la Universidad de San Diego, California, y ha sido permanentemente continuado por voluntarios a través de todo el mundo. Squid, un sistema muy trabajado, puede funcionar como Servidor Intermediario (Proxy) y caché de contenido de Red para los protocolos HTTP, FTP, Gopher y WAIS, Proxy de SSL, caché transparente, caché de consultas DNS y otras como filtros de dominios y control de acceso por IP, MAC y por usuario. Provee potentes opciones para tener un completo control sobre los sitios que se visitan, así como para filtrar, permitir o bloquear el acceso de determinados equipos, IP's, dominios, en las últimas versiones viene con soporte IPv6. En sus inicios fue solo concebido para toda una diversidad de sistemas UNIX-like, pero en los últimos años se han confeccionado versiones para los sistemas de Microsoft.

Instalar Squid en FreeBSD es tarea sencilla utilizando la colección de Ports, esto sería:

```
# cd /usr/ports/www/squid  
# make config ; make install
```

En este proceso será necesario marcar algunas opciones de configuración. Luego para configurarlo se debe editar el fichero */usr/local/etc/squid/squid.conf*:

```
# cd /usr/local/etc/squid/  
# cp squid.conf.default squid.conf squid -z  
# ee squid.conf
```

```
#####CONFIG START  
http_port 8080  
...  
...  
cache_mem 8 MB  
maximum_object_size 50960 KB  
maximum_object_size_in_memory 16 KB  
cache_dir ufs /var/cache 80000 16 256  
...  
cache_access_log /var/log/access.log  
cache_log /var/log/cache.log  
cache_store_log /var/log/store.log  
pid_filename /var/logs/squid.pid  
...  
## ACL SECTION START  
...  
## ACL SECTION END  
...  
tcp_access allow all  
cache_mgr you@somedomain.com  
cache_effective_user squid  
cache_effective_group squid  
visible_hostname proxy.icm.cu  
cachemgr_passwd secret all  
...  
#####CONFIG END
```

Crear el caché de Squid y configurar el inicio en el fichero *rc.conf*, y arrancar el servicio:

```
# squid -z  
# echo 'squid_enable="YES"' >> /etc/rc.conf  
# /usr/local/rc.d/squid start
```

### 3.4.3.2.1. Configuración de jerárquica de proxies.

Squid permite la integración con otros servidores proxies, utilizando esquemas jerárquicos [M] de caché verticales (más simple, suelen llamarse proxies en cascada) u horizontales (más complejo pues utiliza protocolos de intercambio de caché como el ICP). En la red ICM se planifica la utilización de un esquema vertical donde participan el servidor proxy Squid instalado en el cortafuegos y el de la red interna que atiende la solicitudes de los usuarios.

En este paso se debe tomar en cuenta que se van a redireccionar (**Fig. 3.11**) todos los pedidos a otro proxy (Squid en el cortafuegos), para esto será necesario definir el proxy padre lo que impedirá que proxy que se está instalando se conecte directo a los servidores, además optimiza el ancho de banda pues utiliza los dos caché.

Para redireccionar todas las solicitudes (por supuesto, es posible combinarlo con los mecanismos de autenticación) a otro proxy sería:

```
cache_peer treville.icm.cu parent 3128 0
acl All src 0/0
never_direct allow All
```

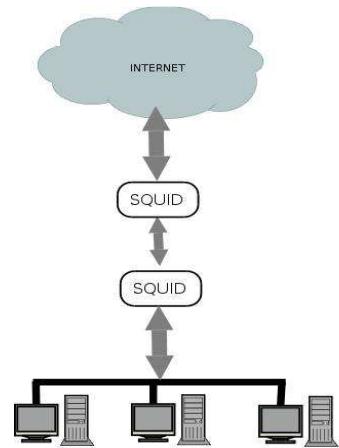


Fig. 3.11 Esquema vertical de proxies Squid.

En este caso lo que el proxy de la red local no encuentre en su caché tratará de pedirlo a su padre y si no obtiene respuesta del padre por algún motivo reportará el error "*cannot forward*" a los usuarios.

### 3.4.3.2.2. Control de acceso y autenticación.

En muchas empresas la razón de ser de una Proxy, además de la optimización de ancho de banda mediante la gestión de la caché, es el control de accesos, por este motivo esto ha sido desde sus inicios un elemento priorizado en Squid, reflejo de este planteamiento son los variados mecanismos que acceso y autenticación (authentication helpers) que oferta a los administradores. Con ellos se puede otorgar acceso a usuarios, máquinas y redes autorizados, negárselo a los no autorizados, restringir accesos a contenidos, redirección o reescritura de las solicitudes, entre otras tareas.

Los controles de acceso en Squid se dividen en dos secciones lógicas. La primera es donde se crean las listas de acceso (ACLs), las cuales pueden estar formadas por máquinas (IP o MAC), redes (IP de red) y mecanismos de autenticación de usuarios mediante identificadores y contraseñas. En la segunda sección se le otorga los permisos a las listas de acceso escritas en la sección anterior permitiendo o denegando el acceso. Los mecanismos de autenticación están identificados por listas de acceso del tipo *proxy\_auth*, de esta forma las aplicaciones clientes envían la información de usuario en las solicitudes (generalmente va en el encabezado, si no está presente Squid la solicita explícitamente), información que es utilizada por Squid para autenticar a estos usuarios y de esta forma otorgar los accesos que correspondan.

### Integración de squid con controladores de dominio.

Un mecanismo muy frecuente en redes de plataformas mixtas gestionadas con controladores de dominio, es el control de autenticación NTLM (NT Lan Manager), un protocolo propietario de autenticación de Microsoft. Esta tarea se simplifica [78a][78b] si se utiliza LDAP (LDAP authentication helpers), pues recordemos que se persigue la idea de que el PDC este soportado sobre FreeBSD con Samba+OpenLDAP, en cuyo caso son posibles otros mecanismos de autenticación propios de los sistemas UNIX-like, pero con esta solución se trata generalizar a un modelo que soporte plataformas mixtas, pues el Directorio Activo de Microsoft es compatible con LDAP v3 por lo que puede ser directamente utilizado para autenticar a los usuarios. Se pueden obtener los mismos resultados utilizando la combinación de Samba con Winbind (caso en que el controlador de dominio porta un Directorio Activo), pero este proceso suele ser más engorroso de configurar [79], pues será necesario que el servidor Squid esté integrado en el dominio.

Para utilizar el autenticador LDAP en Squid se debe tener en cuenta a la hora de instalar el Port de FreeBSD. Autenticar usuario/contraseña contra un controlador de dominio tendría como primer paso configurar el fichero */usr/local/etc/squid/squid.conf* y modificar la sección de *auth\_param* (Etiqueta *auth\_param*) para utilizar el autenticador *squid\_ldap\_auth* de la siguiente forma:

```
...
## ACL SECTION START

auth_param basic program /usr/lib/squid/squid_ldap_auth -R \
-b "dc=icm,dc=cu" \
-D "cn=Administrator,cn=Users,dc=icm,dc=cu" \
-w "password" -f sAMAccountName=%s -h 127.0.0.1
auth_param basic children 5
auth_param basic realm Squid en ICM
auth_param basic credentialsttl 5 minutes
```

Esta variante sólo autentica a los usuarios (esto permite general trazas de los accesos y el tiempo de navegación de cada usuario), pero depende de las listas de control de acceso definir quienes tienen acceso a que recurso (para esto se sugiere estudiar a profundidad los mecanismos de ACLs en Squid), por ejemplo las ACL para esta autenticación quedarían:

```
acl lan proxy_auth REQUIRED src 192.168.2.0/24
...
http_access allow lan
http_access deny all
...
## ACL SECTION END
...
```

Es posible utilizar grupos de usuarios para definir el acceso, para esto será necesario que estén habilitados los grupos en el PDC. Quedaría:

```
...
## ACL SECTION START
...
ldap_auth_program /usr/lib/squid/group_ldap_auth \
-b dc=icm,dc=cu \
-p 636 \
-g distinguishedName \
-d CN=lookup,OU=Services,OU=Users,DC=icm,DC=cu \
-w lookup \
-u cn \
-m member \
-o group \
-S \
-l /var/log/squid/ldaplog \
-h 127.0.0.1
acl inform ldap_auth static 'CN=informatica,OU=Groups,dc=icm,dc=cu'
acl admin ldap_auth static 'CN=admin,OU=Groups,dc=icm,dc=cu'
acl desart ldap_auth static 'CN=desart,OU=Groups,dc=icm,dc=cu'
acl direc ldap_auth static 'CN=derec,OU=Groups,dc=icm,dc=cu'

http_access allow inform
http_access allow admin
http_access allow desart
http_access allow direc
http_access deny all
...
## ACL SECTION END
...
```

### 3.4.3.2.3. Generación y análisis de trazas.

Los logs en Squid son fuente valiosa de información de carga de trabajo y rendimiento, no solo registran información de acceso, registran también errores de configuración y consumo de recursos (Ej. memoria y disco). Squid está capacitado para mantener varios logs, alguno incluso vienen preconfigurados en la instalación del sistema.

Un administrador de Squid debe tener dispuestos todos los mecanismos de precaución para mantener los log salvados de forma segura, pues estos logs, especialmente el de acceso, por su naturaleza están sujetos a protocolos de privacidad que deben ser respetados. Esta información debe ser conservada, pero de ningún modo públicamente, el personal autorizado al acceso de esta información debe ser un grupo bien reducido.

En Squid la generación de trazas queda reflejada igualmente en una sección del fichero de configuración, donde se especifican los archivos que recogerán los logs:

```
...
cache_access_log /var/log/access.log
cache_log /var/log/cache.log
cache_store_log /var/log/store.log
...
```

Generalmente, de los logs generados por Squid el que más llama la atención para ser analizado [80] es el de acceso *access.log*, pues es este log el que registra toda la información de utilidad referente a la actividad de los usuarios y los recursos accedidos desde las redes internas. Por tal motivo este, como el resto de los logs, debe ser mantenido y rotado, para ello es posible usar mecanismos propios de Squid como el comando "*squid -k rotate*", el que puede ser además utilizado en la configuración de tareas periódicas. También es posible habilitar la rotación con programas externos como el *newsyslog* o el *logrotate*.

Existen actualmente aplicaciones para el análisis de los logs accesos de Squid. Una de las más conocidas es MySAR ("MySQL Squid Access Report") [81]. Esta aplicación se integra con Squid y con MySQL y consta de dos partes: una interfaz web (confeccionada con PHP) donde organiza la información a modo de reportes (**Fig. 3.12**) de los registros de accesos y una interfaz de línea de comando (confeccionada en PHP) diseñada para ser integrada con la gestión periódica de tareas del sistema que genera los reportes.

**MySQL Squid Access Report 2.1.4**

[ Home | Administration ]

[ <<< Back to "Daily Summary" | Refresh this page ]

**Hosts and Users Summary for a Specific Day**

<<< Friday, 17 August 2007 >>>

[ Go to today ]

[ Sites Summary for a Specific Day ]

[ Set this view as the default ]

HOST	USERNAME	SITES	BYTES	CACHE PERCENT
Proxy	-	21	5040632	0%
Prueba	-	12	1422214	0%
mmmm	-	31	2483576	0%
<b>TOTALS</b>	<b>3</b>	<b>1</b>	<b>8946422</b>	

**Latest user activity**

HOST IP	USERNAME	TIME	BYTES	URL	STATUS
10.78.32.4	-	11:45:33	494	http://www.google-analytics.com/__utm.gif?	TCP_MISS/200
10.78.32.4	-	11:45:33	362	http://www.friv.com/site/fishtales.swf	TCP_IMS_HIT/304
10.78.32.4	-	11:45:33	355	http://www.friv.com/site/fishtales.html	TCP_IMS_HIT/304
10.78.32.4	-	11:45:25	364	http://e1.extreme-dm.com/s10.g?	TCP_MISS/304
10.78.32.4	-	11:45:25	355	http://www.friv.com/	TCP_IMS_HIT/304

Current active users: 2  
 Current date and time is: 16-11-2008 20:03:36  
 Last processed record: 17-08-2007 11:45:33  
 Number of records processed at last import: 778  
 Last clean-up of the database was done at: 17-08-2007

MySQL Squid Access Report 2.1.4 (c) 2004-2005 by Giannis Stalis  
 Licenced under the GNU General Public Licence.

Fig. 3.12 Reporte de accesos de Squid generado por MySAR.

#### 3.4.3.2.4. Monitoreo y control restricciones.

La mejor manera de distinguir si Squid está funcionando correctamente es por medio del monitoreo [82]. Saber si Squid cuenta con la memoria o el espacio en disco necesario, saber la razón de la navegación lenta, o fallos en el acceso a recursos, intentos de accesos ilegales al proxy, todo esta información y mucha más se obtiene a través de tres vías distintas: registros de *cache.log*, el administrador de caché (*cache manager*), las interfaces SNMP (SNMP MIB).

Respecto al control de restricciones tampoco debemos preocuparnos, pues además de los mecanismos que oferta Squid nativamente, existen también paquetes para desempeñar esta tarea. Uno de ellos es el SquidGuard [83], un sistema de redirección de URLs que protege a Squid con mecanismos de listas negras. Otro ejemplo de estos sistemas es el Squish [84], entre varias funciones brinda un sistema de cuotas por tiempo y volumen de uso de Internet, que puede ser configurada por usuario y por maquina. Finalmente, otra de las herramientas útiles con Squid es el Dansguardian, un antivirus que filtra el contenido que pasa por Squid, previendo la entrada de virus, troyanos, y códigos malintencionados en general.

#### 3.4.4. Servidor de almacenamiento y salva.

Otra prestación para la que resulta necesario encontrar una alternativa de migración es para el almacenamiento de volúmenes de información y gestión de salva con el objetivo de relevar de esta tarea al actual controlador de dominio, el cual, como se mencionó en el Capítulo 1, brinda este servicio tan necesario en el centro.

En la búsqueda de solución para esta problemática se han tenido en cuenta varías alternativas, sobretodo partiendo de la necesidad de encontrar una opción compatible con una red de plataformas mixtas y que no introduzca dificultades para su uso. Por lo que se ha llegado al consenso de que la oferta más clara para este propósito es la utilización de las implementaciones gratuitas de los protocolos de Microsoft para compartir recursos en redes SMB. Basado es esta idea se han encontrado soluciones que ofrecen estos y otros servicios de forma integra y organizada.

Existen distribuciones GNU/Linux y FreeBSD respectivamente que trabaja sobre estos escenarios. Su mayor ventaja es que pueden aprovechar hardware obsoleto donde se dificulta la instalación de un sistema operativo de escritorio de escritorio y convertirlas en ordenadores de altos rendimiento con versiones reducidas de sistemas dedicados con servicios especializados.

Ejemplos de estas distribuciones tenemos a OperFiler con kernel Linux y FreeNAS, el candidato seleccionado, con kernel BSD. Con ediciones de estos sistemas se pueden lograr a muy bajo costo servidores NAS (Network-Attached Storage) para compartir música, multimedia, instalaciones, así como realizar tareas de salvas sincronizadas y servicios FTP de redes locales.

### 3.4.4.1. Presentación de FreeNAS.

**FreeNAS** es un sistema operativo basado en m0n0wall, y por ende basado en FreeBSD. Este proyecto consiste en reemplazar las aplicaciones y herramientas de cortafuego convirtiendo sus funciones básicas en los servicios de almacenamiento en red NAS (*Almacenamiento Conectado en Red*) [85].

Este sistema operativo gratuito, software libre y de código abierto (licencia BSD) permite convertir un ordenador (particularmente ordenadores de pocos recursos de hardware) en un soporte de almacenamiento accesible desde red, por ejemplo para almacenamientos masivos de información, multimedia, salvas, etc. Actualmente FreeNAS se ha convertido en un fuerte competidor de productos comerciales para este tipo de servicios entre los que están Drobo [86], Buffalo [87] y otros.

El software está basado totalmente en FreeBSD, Samba y PHP. El sistema operativo presta soporte a varios modelos de RAID y al igual que su antecesor, *m0n0wall*, es administrable desde una atractiva y organizada interfaz web. Puede ser accedido desde diversas plataformas como Windows, MacOSX, Linux (UNIX-like en general) entre otros dando soporte a servicios de CIF, FTP, NFS y muchos otros. Se destaca por los bajos requerimientos de hardware y la compatibilidad buena cantidad con estándares del mercado [88]. Su instalación utiliza solo unas decenas de MB y puede ser instalado tanto en discos duros como en medios removibles.

#### Características principales

El proyecto FreeNAS es relativamente joven, Oliver Cochard fue quien le dio inicio tomando porciones de m0n0wall tanto de la documentación como del código fuente. Aún ahora el equipo de desarrollo es muy pequeño y las actualizaciones, soporte de hardware, traducciones, corrección de errores, etc., son un tanto demoradas, pero el equipo fuerte y cada versión trae un buen conjunto de significativas y nuevas prestaciones. Aún no alcanza la versión 1.0 (versión en que muchos productos se consideran maduros y aceptados) y no se sabe aún cuando se liberará, ni el equipo de desarrolladores se atreve a decir una fecha, lo que si piden es colaboración y que se sumen al proyecto más desarrolladores. Indudablemente FreeNAS está en sus fases iniciales, sin embargo ya es totalmente utilizable, con reconocidas estadísticas de rendimiento y se encuentra en versión Beta la muy prometedora versión 0.7 (brindará todo el soporte de hardware de la reciente versión de FreeBSD 7.0) que entre sus cualidades particulares se presta especial atención al soporte del renombrado ZFS [89] el sistema de ficheros diseñado por Sun Microsystems para el sistema operativo Solaris el que para muchos especialistas marca una nueva generación en la concepción de sistemas de ficheros.

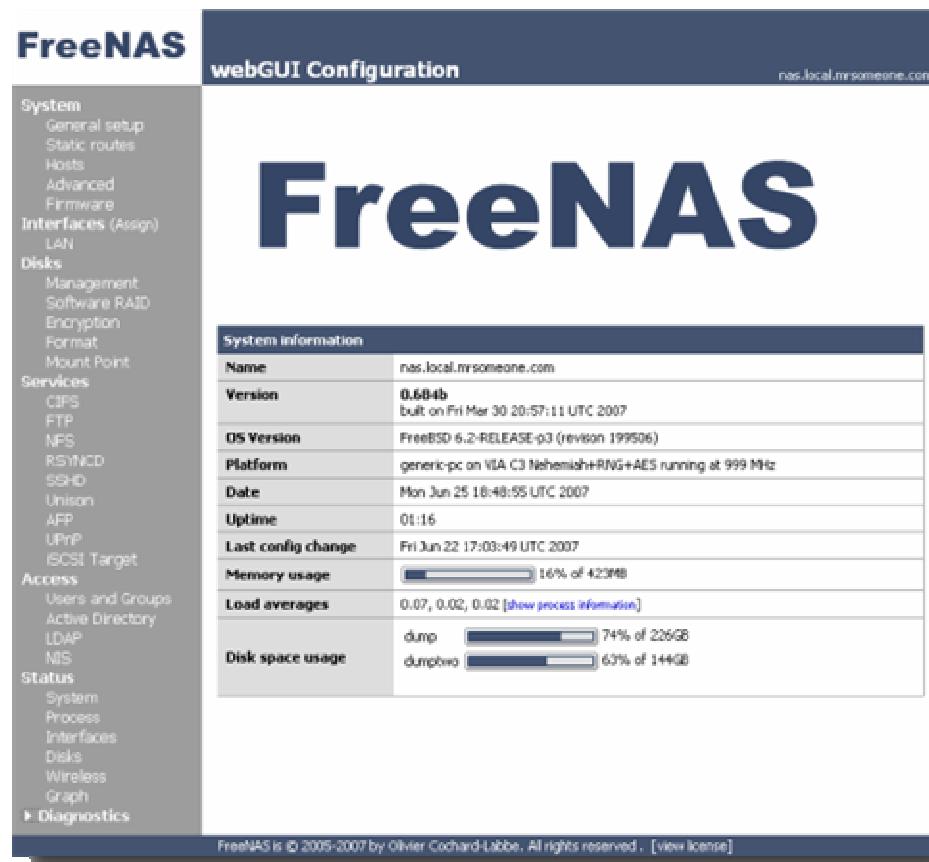


Fig. 3.13 Panel de administración web de FreeNAS.

Una de las cuestiones que ha sido prioritaria en el desarrollo de FreeNAS es su facilidad de uso, cuestión que se ha tenido en cuenta para organizar la interfaz de administración web (**Fig. 3.13**) desde la cual se puede realizar todas las tareas básicas de administración de los servicios y prestaciones. Aunque la administración web puede bastar para administrar el sistema completo, FreeNAS brinda para administradores más experimentados, aquellos que les gustan tener un control más personalizado, el acceso a la línea de comandos la que puede ser accedida localmente desde el teclado, remotamente vía SSH o por la consola disponible en el puerto serie (vía de acceso seguro) del ordenador, forma que no es tan necesaria en servidores de este tipo. Es posible utilizarlo como sistema empotrado, por lógica muy compacto y eficiente, incluso en la modalidad instalada en disco. Es un sistema enfocado estrictamente en las prestaciones NAS, de modo que una vez instalado en una PC la convierte en un NAS dedicado y no podrá desempeñar otras tareas, aunque se puede destacar que el conjunto de tareas que puede desempeñar un NAS suele aumentar a medida que mejoran las tecnologías tanto en software como hardware.

Las versiones más recientes de FreeNAS implementan avanzadas características entre las que vale destacar el uso de disímiles protocolos de red:

- CIFS, protocolo utilizado para la compartir recursos en los sistemas operativos Windows, en los sistemas UNIX-like este protocolo es implementado a través de Samba.
- FTP, el ya muy conocido protocolo de intercambio de ficheros sobre redes IP.
- NFS, el sistema de ficheros de red utilizado para la compartir ficheros en los sistemas UNIX, equivalente a CIFS en entornos Windows.
- RSYNC, protocolo multiplataforma de copias sincronizadas o incrementales, suele utilizarse en soluciones de copias de respaldo, aunque su uso es mucho mas extendido que esto.
- SSHD, se utiliza para administrar los protocolos de copia seguros como la transferencia de ficheros con SFTP y la copia con SCP.
- Unison, herramienta multiplataforma de sincronización de ficheros, mantiene sincronizado bajo diferentes criterios ficheros y directorios.
- AFP, permite el acceso a recursos compartidos de almacenamiento a los usuarios de MacOSX, implementando los servicios de ficheros Netatalk 2.03.

Otras características destacadas de FreeNAS debido a la utilidad de sus prestaciones son:

- Soporte para S.M.A.R.T y otras herramientas de diagnóstico de discos duros.
- Compatibilidad con las tecnologías iSCSI, una combinación de la arquitectura robusta de SCSI con la versatilidad de serial ATA.
- Software RAID:
  - RAID 0 con gstripe/gvnum
  - RAID 1 con gmirrror/gvnum
  - RAID 5 con graid5 experimental y gvnum
  - RAID Avanzado: 1+0, 0+1, 5+1, etc.
- Encriptación de disco con geli (automatizado con scripts).
- Soporte para ZFS, mencionado anteriormente, actualmente en fase de prueba en versiones Beta de la 0.7.
- Autenticación de usuarios ya sea local o integrada con controladores de dominios (Directorios Activos de servidores Windows como caso particular).
- Sistema de manejo de trazas centralizado. FreeNAS trae el sistema Syslogng que ayuda a complementar su función como servidor de salva, permitiendo almacenar las salvas de los logs de otros servidores.

Al ser FreeNAS heredero directo de m0n0wall su instalación es muy similar a la de pfSense, vista en el capítulo anterior. A diferencia de pfSense, el equipo de desarrollo de FreeNAS ha velado por mantener el proyecto bien documentado, motivando, de esta forma también, a los usuarios finales a generar documentación basada en sus pruebas con el producto, ejemplo de esta documentación son algunos artículos [90a][90b][90c][90d] publicados en Internet donde los autores nos muestran en proceso detallado para instalar y configurar FreeNAS, estos artículos vienen acompañados de capturas de pantalla para cada uno de los pasos de la instalación.

Otros artículos o documentos sugerentes en la comprensión y aprendizaje de la utilización de FreeNAS los podemos encontrar en el sitio de FreeNAS estos son "*FreeNAS Quick Start Guide*" y "*FreeNAS Setup and User guide*" quienes conjuntamente con el libro "*Learning FreeNAS*" de Gary Sims nos podrían dar una formación bastante fundamentada respecto al tema.

### 3.4.4.2. Selección del Hardware.

Cuando se planea el montaje de un NAS inciden varios factores, el primero de ellos sería la disponibilidad de recursos (equipos o servidor o el presupuesto para la compra de equipamiento afín). Nunca se debe despreciar la capacidad de disco de un NAS, pues en este frecuentemente se almacena multimedia, software, correos, salvas y toda una creciente lista de contenidos, con los que las tasas de consumo de disco va también en aumento, contando también con que toda esta información debe estar respaldada (como caso mínimo un RAID espejo, caso ideal un servidor réplica).

La selección de hardware para la implantación del servidor FreeNAS no es tarea difícil pues, como se menciona anteriormente, los requerimientos de hardware son bastante bajos. En el Instituto esta tarea se ha simplificado, aún más, gracias a la migración de los antiguos servidores, pues gracias a ello, se puede reaprovechar el actual controlador de dominio. Este equipo no solo encaja con el perfil de requerimientos, sino que es la opción ideal entre otras alternativas, pues las características de este servidor, además de ser una servidor profesional, lo enfocan como servidor de ficheros, y en la idoneidad van tanto el hardware como el chasis del servidor. El hardware está compuesto por una motherboard Asus CUV4X-DLS, dual PIII, 1G RAM y un arreglo de discos fijos SCSI, además se tiene previsto incorporar tarjetas de expansión controladora de RAID por hardware(**Fig. 3.14**), actualmente el instituto cuenta con una de estas para pruebas y en caso de éxito se pueden adquirir algunas otras. El chasis es un EN8950 con el que muestra la figura (**Fig. 3.15**). Además en el **Anexo II.G** se pueden apreciar las especificaciones técnicas de los componentes de este servidor.



Fig. 3.15 Torre EN8950 para servidores NAS.

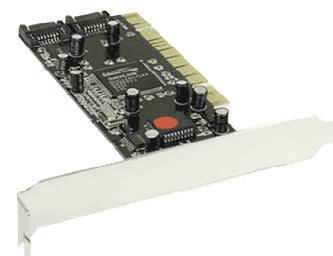


Fig. 3.14 Tarjeta PCI controladora RAID.

## Conclusiones

Finalmente se le da conclusiones a esta tesis y siendo realistas y autocráticos se debe admitir que distan aún las conclusiones de este proyecto. Un proyecto, en la práctica, adopta muchos matices, los que en ocasiones se tornan difíciles de recoger en una tesis, por extensa que sea. Sin embargo es meritorio admitir que se ha tratado de ser exhaustivos, dándole al menos una variante de solución a cada uno de los problemas abordados. Se puede destacar que las soluciones (al menos en el plano teórico) representan eficiencia, esto respaldado con volúmenes de experimentada bibliografía desprendida de la práctica.

Se ha obtenido un rediseño de red, flexible, extensible, seguro, robusto cumpliendo los parámetros básicos que catalogan como una red fiable [C], amén del conjunto de modificaciones y la introducción de pfSense como cortafuegos de red, brindando soporte a cientos de prestaciones que respaldan estas características. Al mismo tiempo se han encontrado variantes de solución a fin de dar respuesta a nuevas prestaciones en la red del Instituto.

En la evaluación de los requerimientos e inversiones se ha sido consecuente con las necesidades, dando estricta respuesta a cada una de las problemáticas citadas. Teniendo en cuenta el reaprovechamiento de la plataforma actual e incorporando la nueva tecnología se espera no solo dar respuesta a las necesidades, también elevar la eficiencia y disponibilidad de los servicios informáticos de la red del ICM al tiempo que se brinda soporte de conectividad al sistema de instituciones de la música.

Se ha confeccionado una guía (con un elevado carácter práctico) de migración al software libre de los servidores y servicios de red vigentes en la red del Instituto. A pesar de ser un guía parcial y concreta, enfocada además al caso específico de la red del ICM, sí es meritorio destacar que representa un primer intento de confección de guía de migración en el marco ministerial y cumple con cientos de parámetros compatibles con la política de migración en las instituciones de cultura.

A manera de resumen se considera que se le ha dado cabal cumplimiento al conjunto de objetivos trazados para esta tesis. Este documento adquiere una categoría de guía en el desarrollo del proyecto en cuestión, siendo significativamente atractivo cumplir al margen de las posibilidades lo que se plantea en el mismo.

## *Recomendaciones*

Como es posible notarlo, ha culminado un extenso y acaparador trabajo donde se han abordado, con carácter más o menos práctico, múltiples temáticas que han ganado mucha popularidad y afición en los últimos tiempos. Es nuestro país un abanderado vanguardista, impulsor por convicción de la filosofía y la tecnología que sustentan a las temáticas que aquí se desarrollan, por tal motivo, representa, para cada uno de los técnicos y los científicos que respaldan el desarrollo informático de este país, un compromiso, el estudio y desarrollo de las tecnologías informáticas relacionadas con el software libre.

Por este motivo se recomienda utilizar esta tesis como pilar de conocimientos para futuras investigaciones. Las líneas de investigación que se desprenden de esta tesis son diversas pero todas apuntan en una dirección común: el software libre. Es posible desarrollar investigaciones sobre seguridad y monitoreo de redes, sobre implantación de sistemas de soluciones integradas, elaborar guías más generales de migración al software libre, hacer investigaciones sobre comparaciones de diferentes sistemas y evaluar diferentes variables, en fin, todo un universo de conocimientos aguarda para todo aquel que encuentre en esta tesis un objeto de estudio.

Entre otras de las aristas que se desprenden de esta tesis pudieran estar los primeros escaños de la objetivación y confección de la política y guía de migración al software libre en las instituciones de cultura, utilizando al Ministerio de Cultura como organismo rector de esta tarea. Una apropiada atención a este proyecto pudiera conducir a un exitoso cumplimiento de la política nacional de migración al software libre por parte del Ministerio de Cultura.

## Bibliografía

### **Libros:**

[A] Software libre para una sociedad libre

Autor: Richard M. Stallman Introducción de Lawrence Lessig

[B] GUÍA CUBANA DE MIGRACIÓN A SOFTWARE LIBRE

Autores: UCI Facultad de Software Libre, Proyecto Unicornio.

[C] SEGURIDAD EN UNIX Y REDES

Autor: Antonio Villalón Huerta

[D] m0n0wall Handbook

Capítulo: What m0n0wall is not (<http://doc.m0n0.ch/handbook/intro-not.html>)

Autores: Manuel Kasper y Chris Buechler

URL: <http://doc.m0n0.ch/handbook/>

[E] Network Administration with FreeBSD 7

Autor: Babak Farrokhi

Buscar: Bridges

[F] Sistema Integral de Seguridad y Acceso a la Red de un departamento de la UPC

Autor: Albert Marques

[G] Building a Server with FreeBSD 7

Autor: Bryan J. Hong

[H] FreeBSD®6 Unleashed

Autor: Brian Tiemann

[I] Técnicas de defensa comunes bajo variantes del sistema operativo Unix.

Autor: Juan Pablo Sarubbi

[J] Samba 4 - Active Directory

Autor: Andrew Bartlett

[K] Samba-3 by Example Second Edition

Autor: John H. Terpstra

[L] Samba: UNIX and NT Networking

Autor: James DeRoest

## Artículos y enlaces:

[M] Squid: The Definitive Guide

Autor: Duane Wessels

[1a] La Definición de Software Libre

URL: <http://www.gnu.org/philosophy/free-sw.es.html>

[1b] Artículos sobre software libre en “En defensa de la humanidad”

URL: <http://www.porlacultura.cult.cu/index.php>

[1c] FLOSS Concept Booklet

URL: [http://en.wikibooks.org/wiki/FLOSS\\_Concept\\_Booklet](http://en.wikibooks.org/wiki/FLOSS_Concept_Booklet)

[2a] Seven Different Linux/BSD Firewalls Reviewed

URL: <http://www.fsckin.com/2007/11/14/7-different-linuxbsd-firewalls-reviewed/>

[2b] Protecting networks with SmoothWall Express

Autor: Joseph R. Baxter

URL: <http://www.linux.com/feature/154568?theme=print>

[2c] Set up your firewall with Firewall Builder

Autor: Ben Martin

URL: <http://www.linux.com/feature/144533?theme=print>

[2d] Using the PF Firewall on FreeBSD

Autor: xylophone

URL: <http://web.irtnog.org/howtos-orig/freebsd-firewall>

[3] URL: <http://es.wikipedia.org/wiki/Backbone>

[4] URL: <http://es.wikipedia.org/wiki/VLAN>

[6] URL: <http://www.bsdinstaller.com/>

[7] FlashHowtoScript

Autor: Chris Buechler

URL <http://devwiki.pfsense.org/FlashHowtoScript>

[8] URL: [http://es.wikipedia.org/wiki/Portal\\_cautivo](http://es.wikipedia.org/wiki/Portal_cautivo) o [http://en.wikipedia.org/wiki/Captive\\_portal](http://en.wikipedia.org/wiki/Captive_portal)

[9] URL: [http://en.wikipedia.org/wiki/Stateful\\_firewall](http://en.wikipedia.org/wiki/Stateful_firewall)

[10] The OpenBSD Packet Filter

URL: <http://www.openbsd.org/faq/pf/>

## Artículos y enlaces:

[11a] Firewall Topologies

URL: [http://www.firewall.cx/firewall\\_topologies.php](http://www.firewall.cx/firewall_topologies.php)

[11b] URL: <http://es.wikipedia.org/wiki/DMZ>

[12] URL: <http://es.wikipedia.org/wiki/SSID>

[13a] URL:

[http://tecun.cimex.com.cu/tecun/software/Soporte%20Tecnico%20de%20Redes/TELINDUS\\_ON\\_EACCESS/Documentos/MINIDSLAM/caso\\_vlan-pvc/2401 ADSL vlan bridging CU.doc](http://tecun.cimex.com.cu/tecun/software/Soporte%20Tecnico%20de%20Redes/TELINDUS_ON_EACCESS/Documentos/MINIDSLAM/caso_vlan-pvc/2401 ADSL vlan bridging CU.doc)

[13b] HOWTO setup vlans with pfSense

URL: [http://doc.pfsense.org/index.php/HOWTO\\_setup\\_vlans\\_with\\_pfSense](http://doc.pfsense.org/index.php/HOWTO_setup_vlans_with_pfSense)

[14] Tutorial sobre pfSense

Autor: Josep Pujadas Jubany

URL: [http://www.bellera.cat/josep/pfsense/index\\_cs.html](http://www.bellera.cat/josep/pfsense/index_cs.html)

[15a] Configuring IPSec VPN Connection between FreeBSD and OpenBSD.

Autor: Cezary Morga

URL: [http://www.bsdguides.org/guides/freebsd/security/ipsec\\_vpn](http://www.bsdguides.org/guides/freebsd/security/ipsec_vpn)

[15b] OpenVPN 2

Autor: Bert JW Regeer

URL: <http://www.bsdguides.org/guides/freebsd/security/openvpn2>

[16] URL: <http://es.wikipedia.org/wiki/Caché>

[17] URL: <http://es.wikipedia.org/wiki/TCP/IP>

[18] Quick start squidGuard package

URL: <http://diskatel.narod.ru/sgquick.htm>

[19] Firewall Failover with pfsync and CARP

Autor: Ryan McBride

URL: <http://www.countersiege.com/doc/pfsync-carp/>

[20b] ASSP With Embedded ClamAV Integrated Into Postfix With Virtual Users And Domains

URL: [http://www.howtoforge.com/download.php?id=2507\\_0](http://www.howtoforge.com/download.php?id=2507_0)

[20c] FreeBSD Install Guide

URL: [http://www.asspsmtp.org/wiki/FreeBSD\\_Install\\_Guide](http://www.asspsmtp.org/wiki/FreeBSD_Install_Guide)

[21] URL: <http://www.bsdi.com>

## Artículos y enlaces:

[22a] URL: <http://uptime.netcraft.com/up/today/top.avg.html>

[22b] URL: <http://www.levenez.com/unix/unix.png>

[23] URL: <http://www.netbsd.org>

[24] URL: <http://www.freebsd.org>

[25] URL: <http://www.openbsd.org>

[26] URL: <http://es.wikipedia.org/wiki/POSIX>

[27] URL: <http://en.wikipedia.org/wiki/Unix-like>

[28] Why FreeBSD

Autor: Frank Pohlmann

URL: <http://www.ibm.com/developerworksopensource/library/os-freebsd/>

[29] URL: [http://en.wikipedia.org/wiki/BSD\\_and\\_GPL\\_licensing](http://en.wikipedia.org/wiki/BSD_and_GPL_licensing)

[30] URL: <http://www.freebsd.org/gallery.html>

[31] URL: <http://www.linux.org/dist>

[32] What's cooking for FreeBSD 7

URL: <http://ivoras.sharanet.org/freebsd/freebsd7.html>

[33] URL: <http://www.freebsd.org/cgi/man.cgi?query=gmirror&sektion=8>

[34] URL: <http://www.freebsd.org/cgi/man.cgi?query=gstripe&sektion=8>

[35] URL: <http://www.freebsd.org/cgi/man.cgi?query=gshsec&sektion=8>

[36] URL: [http://www.freebsd.org/doc/en\\_US.ISO8859-1/books/handbook/mac.html](http://www.freebsd.org/doc/en_US.ISO8859-1/books/handbook/mac.html)

[37] Pluggable Authentication Modules

Autor: Dag-Erling Smørgrav

URL: [http://www.freebsd.org/doc/en\\_US.ISO8859-1/articles/pam/](http://www.freebsd.org/doc/en_US.ISO8859-1/articles/pam/)

[38] FreeBSD Release Engineering

Murray Stokely

URL: [http://www.freebsd.org/doc/en\\_US.ISO8859-1/articles/releng/](http://www.freebsd.org/doc/en_US.ISO8859-1/articles/releng/)

## Artículos y enlaces:

[39] FreeBSD Security Information

URL: <http://www.FreeBSD.org/security/>

[40] FreeBSD VuXML

Autor: Jacques Vidrine

URL: <http://www.vuxml.org/freebsd/>

[41] URL:

<http://www.freebsd.org/cgi/man.cgi?query=portaudit&sektion=1&apropos=0&manpath=FreeBSD+7.0-RELEASE+and+Ports>

[42] URL: <http://www.freebsd.org/cgi/man.cgi?query=jail&sektion=8>

[43] URL: <http://www.freebsd.org/cgi/man.cgi?query=chflags&sektion=1>

[44] URL: <http://m0n0.ch/wall/>

[45] URL: <http://www.pfsense.org/>

[46] URL: <http://www.freenas.org/>

[47] URL: <http://www.desktopbsd.net/>

[48] URL: <http://www.pcbsd.org/>

[49] URL: <http://www.truebsd.org/>

[50] URL: <http://www.rofreesbie.org/>

[51] URL: <http://www.freesbie.org/>

[52] URL: <http://frenzy.org.ua/eng/>

[53] URL: <http://www.damnsmallbsd.org/>

[54] URL: <http://www.askozia.com/pbx>

[55] Why (almost) every Web site needs an RDBMS

Autor: David Mertz, Ph.D

URL: <http://www.ibm.com>

[56] URL: <http://www.proftpd.org>

[57] URL: <http://www.freebsd.org/doc/en/books/handbook/linuxemu-oracle.html>

## Artículos y enlaces:

[58] URL: <http://wiki.exim.org/>

[59] URL: <http://www.courier-mta.org/authlib/documentation.html>

[60] URL: <http://www.courier-mta.org/imap/documentation.html>

[61] Eleven Examples for Configuring Exim

Autor: Philip Hazel

URL: [http://www.oreillynet.com/pub/a/oreilly/networking/news/exim\\_0701.html](http://www.oreillynet.com/pub/a/oreilly/networking/news/exim_0701.html)

[62a] URL: <http://www.squirrelmail.org>

[62a] URL: <http://sourceforge.net/projects/squirrelmail>

[63] URL: <http://es.wikipedia.org/wiki/Intranet>

[64] URL: [http://es.wikipedia.org/wiki/Network\\_Information\\_Service](http://es.wikipedia.org/wiki/Network_Information_Service)

[65] URL: <http://www.aplicacionesempresariales.com/el-servidor-de-archivos-samba.html>

[66] URL: <http://websvn.samba.org/cgi-bin/viewcvs.cgi/trunk/samba4-ad-thesis/?root=lorikeet>

[67] Setting up A Samba Server with Windows XP Clients

URL: <https://www.ccs.uky.edu/docs/samba.htm>

[68a] Integración de redes con OpenLDAP, Samba, CUPS y PyKota

Autor: Sergio González González

URL: <http://olsacupy.berlios.de/v0.2/ldap-samba-cups-pykota-v0.2.html>

[68b] Setting up a Samba 3 primary domain controller and file/print/software deployment server, using Debian 4.0 Etch

URL: <http://thegoldenear.org/toolbox/unices/samba-3-pdc-print-server-debian-etch.html>

[68c] Curso de integración de Sistemas Linux/Windows

URL: [http://www.ispcmw.rimed.cu/sitios/digbiblio/cont/EI/SO\\_Linux/mas\\_sw/integracion-linwin.pdf](http://www.ispcmw.rimed.cu/sitios/digbiblio/cont/EI/SO_Linux/mas_sw/integracion-linwin.pdf)

[69] URL: [https://www.bsdwiki.de/FreeBSD - Samba\\_PDC](https://www.bsdwiki.de/FreeBSD - Samba_PDC)

[70] Build a Samba PDC with LDAP backend

URL: [http://www.bsdguides.org/guides/freebsd/networking/samba\\_pdc\\_ldap](http://www.bsdguides.org/guides/freebsd/networking/samba_pdc_ldap)

[71] URL: [http://en.wikipedia.org/wiki/List\\_of\\_AMP\\_packages](http://en.wikipedia.org/wiki/List_of_AMP_packages)

## Artículos y enlaces:

[72] URL: <http://blog.cbhacker.com/2008/09/setting-up-a-lamp-server-on-freebsd/>

[73] URL: <http://www.joomla.org/>

[74] URL: <http://www.mamboserver.com/>

[75] URL: <http://drupal.org/>

[76] URL: <http://wordpress.org/>

[77] URL: <http://www.oscommerce.com/>

[78a] Configuring Squid on Linux to authenticate with Active Directory  
URL:

<http://www.papercut.com/kb/Main/ConfiguringSquidProxyToAuthenticateWithActiveDirectory?action=print>

[78b] Configure squid for LDAP authentication using squid\_ldap\_auth helper

Autor: Vivek Gite

URL: <http://www.cyberciti.biz/tips/howto-configure-squid-ldap-authentication.html>

[79] Autentificar squid contra Active Directory

Autor: Yadrian Moreno Rodriguez

URL

[http://www.vcl.jovenclub.cu/munic/remedios/index2.php?option=com\\_content&task=view&id=32&pop=1&page=0&Itemid=53#](http://www.vcl.jovenclub.cu/munic/remedios/index2.php?option=com_content&task=view&id=32&pop=1&page=0&Itemid=53#)

[80] Squid Proxy Sever View logs / log files

Autor: Vivek Gite

URL: <http://www.cyberciti.biz/faq/howto-linux-unix-view-squid-log-files/>

[81] URL: <http://giannis.stoilis.gr/software/mysar/>

[82] URL: <http://www.visolve.com/squid/whitepapers/monitoringsquid.pdf>

[83] URL: <http://www.squidguard.org/>

[84] URL: <http://www.ledge.co.za/software/squint/squish/>

[85] URL: <http://www.learnfreenas.com/modules/smartaFAQ/faq.php?faqid=2>

[86] URL: <http://www.drobo.com/>

[87] URL: <http://www.buffalotech.com/>

## Artículos y enlaces:

[88] freenas\_users\_hardware

URL:

[http://www.freenas.org/index.php?option=com\\_openwiki&Itemid=30&id=freenas\\_users\\_hardware](http://www.freenas.org/index.php?option=com_openwiki&Itemid=30&id=freenas_users_hardware)

[89] URL: <http://www.learnfreenas.com/modules/smartyfaq/faq.php?faqid=5>

[90a] Building a Home File Server with FreeNAS ( FreeBSD based NAS Server )

Autor: Vivek Gite

URL: <http://www.cyberciti.biz/tips/low-cost-home-media-file-server.html>

[90b] Quick and Easy NAS using FreeNAS

URL: <http://www.netadmintools.com/art503.html>

[90c] Network-Attached Storage with FreeNAS

Autor: Falko Timme

URL: [http://www.howtoforge.com/network\\_attached\\_storage\\_with\\_freenas](http://www.howtoforge.com/network_attached_storage_with_freenas)

[90d] HOWTO: Install FreeNAS

URL: [http://developer.novell.com/wiki/index.php/HOWTO:\\_Install\\_FreeNAS](http://developer.novell.com/wiki/index.php/HOWTO:_Install_FreeNAS)

# Anexo I.A

## Gráficos de rendimiento y tráfico en un cortafuegos pfSense.

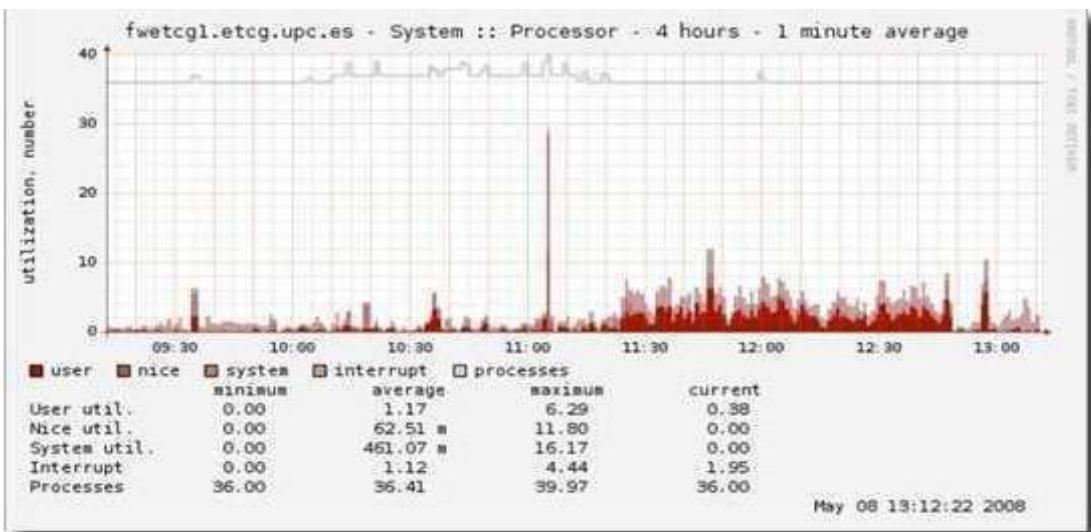


Gráfico de uso del procesador y rendimiento del sistema.

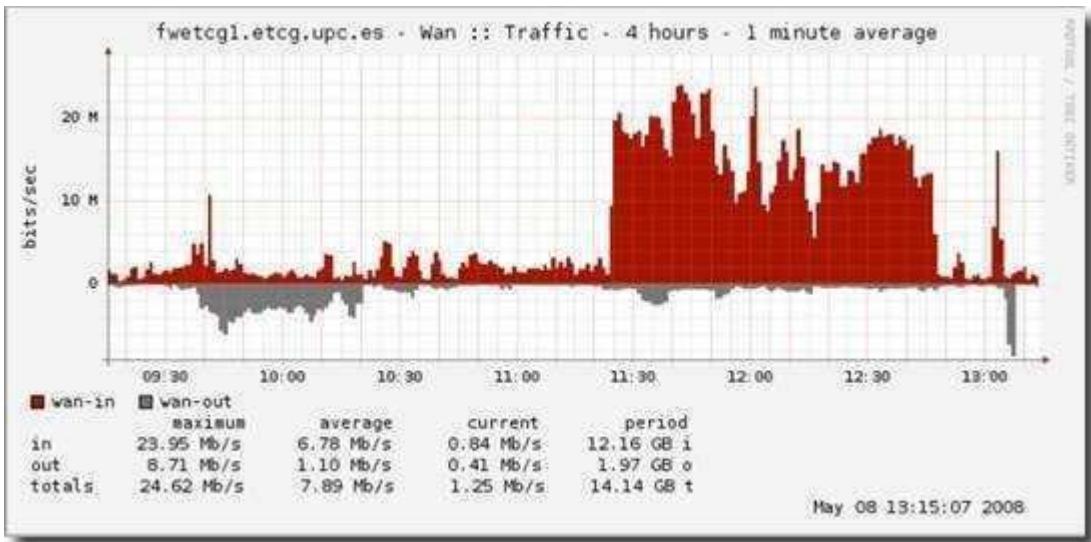


Gráfico de valores de tráfico diario

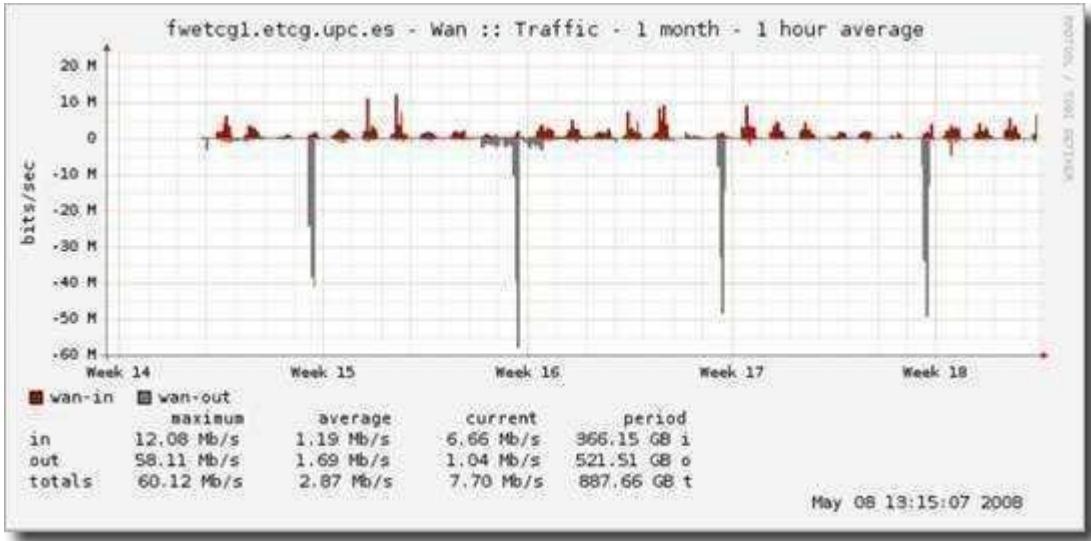
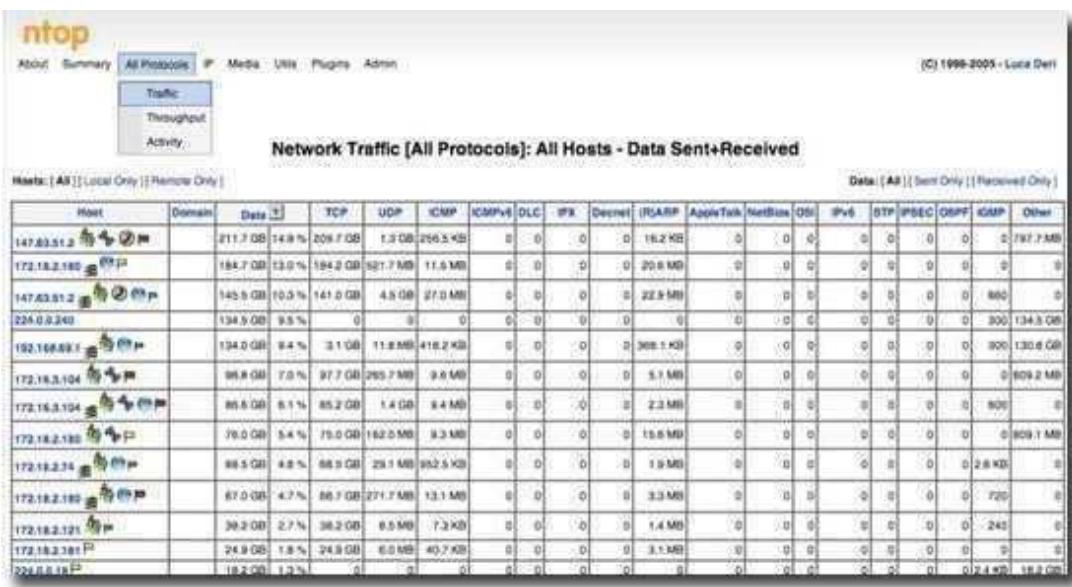


Gráfico de valores de tráfico mensual.

# Anexo I.B

## Sistemas de monitoreo de redes.

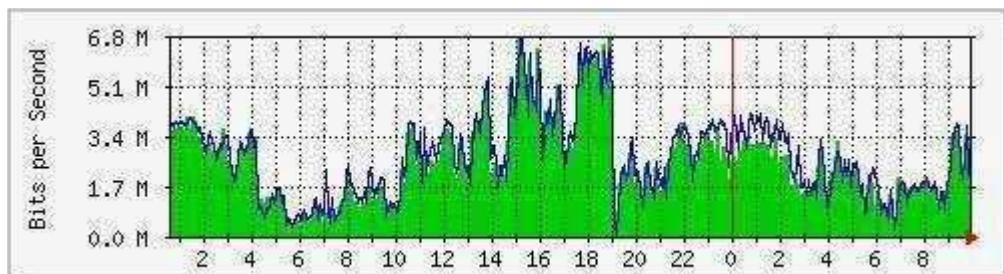


## Panel de control web de ntop

```
notwist@notwist:~$ nmap localhost
Starting Nmap 4.20 ( http://insecure.org ) at 2007-04-02 15:50 CEST
Interesting ports on localhost (127.0.0.1):
Not shown: 1691 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
631/tcp   open  ipp
3306/tcp  open  mysql

Nmap finished: 1 IP address (1 host up) scanned in 0.213 seconds
notwist@notwist:~$
```

## Utilización de **nmap** desde la consola de comandos



## Gráfico de consumo de ancho de banda generado por un MRTG



Vista del panel de control de Nagios

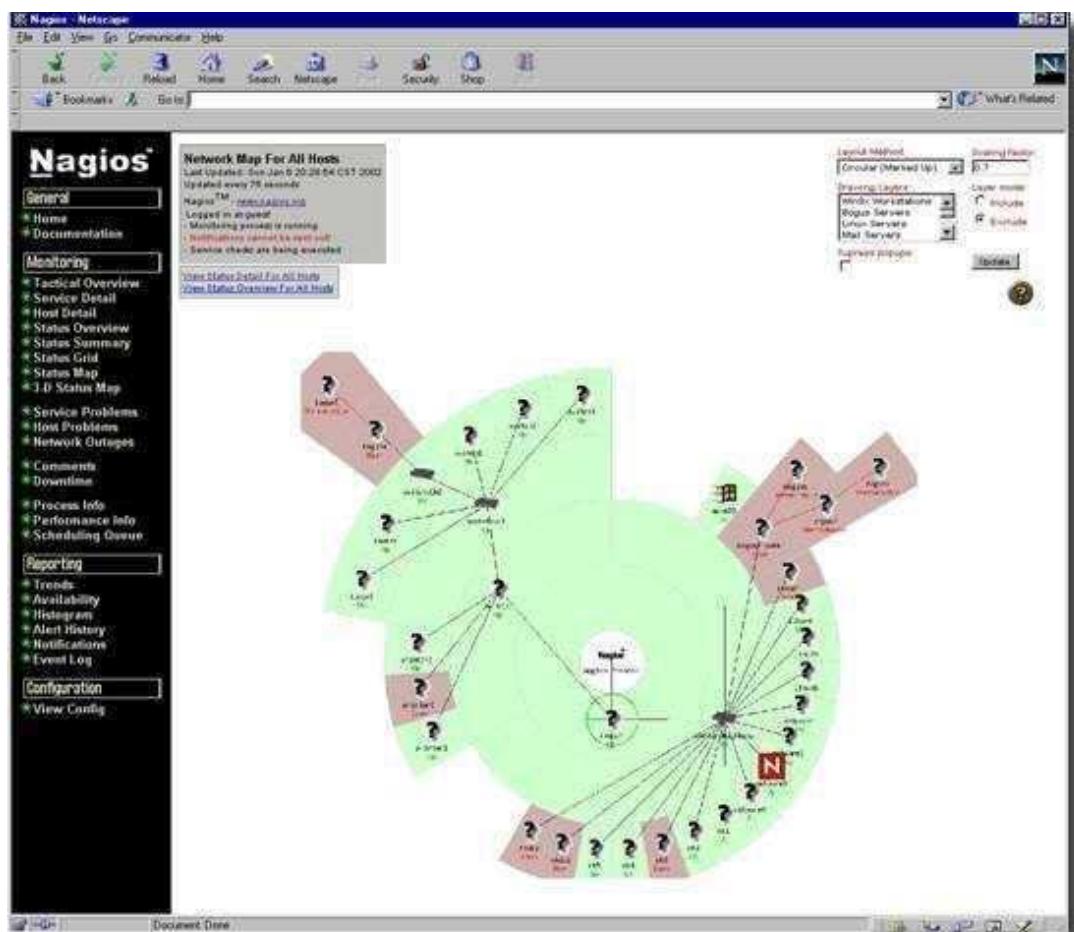


Gráfico de distribución de redes generado por Nagios

# Anexo II.A

## Propuesta de equipamiento para enrutador-cortafuegos.

# **FX5622 INTEL Celeron M 1Ghz 8 NIC Firewall/Router Platform**

## **4 Intel GigaLAN + 4 Intel 10/100**



1Ghz Celeron-M Multi-LAN system with 8 Intel LAN's (4 Gigabit and 4 10/100), 1 Serial (RS232), 2 USB and 1 mini-PCI. The system has an onboard bootable Compact Flash slot and space to install a 2.5" SATA Hard Drive.



### **Features:**

- Fanless and low power consumption design
- Intel Celeron-M 1GHz CPU
- 1GB RAM Installed
- 8 LAN's
- 2 x USB 2.0
- One Compact Flash Slot
- One 2.5" SATA HDD Space

### **Specifications:**

- CPU Board: Intel Celeron-M 1Ghz CPU with 1GB DDR2-RAM Installed - Upgradeable to 2GB RAM
- Chipset: Intel 82910GMLE
- I/O Outlets:
  - 8 RJ45 connectors (4 x Intel 82551 Chipset 10/100 and 4 x Intel 82573 chipset 100/1000)
  - 2 USB connectors
  - 1 RS-232 connector
  - 1 Reset Button
  - 1 Dc-In connector
- Storage Bays: 1 x 2.5" SATA HDD Space and 1 x Compact Flash Slot
- Watchdog Timer
- LAN Bypass Function: LAN3/LAN4
- Power Requirements: DC 9V 4A ~ 28V 1.3A Input (19V 3.42A AC/DC adapter supplied)
- Operating Temp.: 0~45 degree C.
- LED Indicators: 1 Power LED, 1 User Defined Status LED, 1 HDD/CF access LED and 16 LAN LED's
- Dimensions: 250mm W x 180mm D x 44mm H
- Supplied Accessories: 1 AC/DC 19V Adapter with AC power cable, 1 2.5" SATA HDD installation kit

## Anexo II.B

Ejemplos de tarjetas de red útiles en la configuración de hardware del cortafuegos.

# Intel® PRO/100 S Server Adapter

*Fast, managed server connections with accelerated LAN security*

## KEY FEATURES

- Advanced features alleviate server bottlenecks while increasing uptime
- Integrated security co-processor increases network performance
- Intel® SingleDriver™ technology simplifies installation and maintenance

The Intel® PRO/100 S Server Adapter represents the next generation of Fast Ethernet server connections. Advanced server features alleviate server bottlenecks and increase uptime, while accelerated LAN security preserves performance on IPSec-enabled networks.



A member of the industry's first complete family of adapters with security  
Intel® PRO/100 S Desktop, Mobile and Server Adapters.

### Intel® 82550 Fast Ethernet Controller with integrated encryption co-processor

Integrated LAN silicon and encryption co-processor boosts network performance and frees system resources by offloading encryption from the server's processor.

### Scalable throughput and high availability

Aggregate bandwidth and establish automatic redundant connections using any combination of Intel® Server Adapters or LOM connections.

### 3DES encryption algorithms

The highest level of security widely available to protect data travelling on IPSec-enabled networks.

# Intel® PRO/1000 XF Server Adapter

*PCI-X fiber Gigabit connection for your next-generation network*

## KEY FEATURES

- Greater distances and noise resistance enabled through fiber-optic connection
- High network performance and flexibility via PCI-X bus at 64-bit/133MHz
- Alleviate server bottlenecks while increasing uptime through advanced server features

Intel's third-generation Gigabit fiber adapter eliminates server bottlenecks with industry-leading Gigabit performance in a PCI-X bus in 64-bit/133MHz and easily integrates into your existing Ethernet infrastructure.



### 1000BASE-SX-fiber connectivity

Deliver data further and with less susceptibility to noise over fiber-optic cabling.

### Cover distances up to 275 meters

Connect campus buildings and department floors with fast, Gigabit networking.

### Noise-resistant networking

Fiber networking is immune to interference in electro-magnetically noisy environments.

### Migrate from ATM or FDDI

Move to Gigabit Ethernet for widely deployed, high-performance networking – the most deployed networking environment.

### Deliver high throughput and lower CPU utilization

Intel® PCI-X Server Adapters are designed to allow you to get the maximum performance from your servers while minimizing CPU utilization. With advanced network services you can scale to multi-Gigabit bandwidth while increasing server availability.

# Intel® PRO/100 S Dual Port Server Adapter

*Two 10/100Mbps ports for added server flexibility, plus accelerated LAN security*

Introducing the industry's first dual port server adapter with accelerated LAN security. With two 10/100 ports, each adapter delivers up to 400Mbps for twice the bandwidth per server slot.

## **NEW! Integrated LAN silicon and encryption co-processor**

Boosts network performance and frees system resources by offloading encryption from the server's processor.

## **Up to three connections per PCI slot**

Team with the Intel® 82550, 82559 or 82558 Onboard LAN controller for an additional resilient connection.

## **Scalable throughput**

Aggregate bandwidth while providing automatic redundant connections to remove network bottlenecks and promote server availability.

## **Simultaneous 10Mbps and 100Mbps**

Run each port independently to support network segments at different speeds.



## **KEY FEATURES**

- Two 10/100Mbps ports on one card
- Advanced features alleviate server bottlenecks while increasing uptime
- Intel® SingleDriver™ technology simplifies installation and maintenance
- High link availability through Adapter Fault Tolerance, PCI Hot Plug\*, and Active PCI\*

# Intel® PRO/1000 XT Server Adapter.

*PCI-X 10/100/1000Mbps copper connection for your next-generation network*

Alleviate server bottlenecks with easy-to-scale Gigabit connectivity, using your existing Cat-5 cabling. Benefit from the reliable, high-performance Intel® PRO/1000 XT Server Adapter, which will automatically sense infrastructure upgrades, and begin running at Gigabit speeds – without reconfiguration. Choose from standard PCI or a low-profile PCI version.

## **1000BASE-T Gigabit Ethernet over copper**

Fight server bottlenecks with Gigabit connectivity using existing Category-5 copper cabling.

## **Flexible 10/100/1000 connectivity**

Deliver Ethernet, Fast Ethernet and Gigabit connectivity to match the devices in an evolving network environment.

## **Easily migrate to Gigabit Ethernet**

Use existing Category-5 copper cabling for the fastest Ethernet speeds at distances up to 100 meters.

## **Reduce multiple network media types**

Make Ethernet the standard in the enterprise – for desktops, laptops, servers and the backbone.

## **Lower IT training costs**

Leverage existing Ethernet knowledge and skills for the entire enterprise.



## **KEY FEATURES**

- Easy, cost-effective migration to Gigabit Ethernet over Category-5 cabling
- High network performance and flexibility via PCI-X bus at 64-bit/133MHz
- Alleviate server bottlenecks while increasing uptime through advanced server features
- Low-profile bracket option available – ideal for high-density, rack-mount servers

# Anexo II.C

## Commutador (switch) capa III con soporte VLAN y Gigabit Ethernet.

# **SWITCH NETGEAR 24PTOS 10/100/1000 GB PORT STACKABLE(GS724TS)**



## **Network Protocol and Standards Compatibility**

- IEEE 802.3 10BASE-T
- IEEE 802.3u 100BASE-TX
- IEEE 802.3ab 1000BASE-T
- IEEE 802.3z 1000BASE-X
- IEEE 802.3x full-duplex flow control

## **Interfaces**

- 24 10/100/1000 Mbps switching ports
- 4 Built-in shared SFP Gigabit Ethernet fiber ports for 100/1000 Mbps connectivity
- Auto-sensing and auto-negotiating capabilities for all copper ports
- Auto Uplink™ on all ports to make the right connection

## **LEDs**

- Unit: Power, Master, Stack ID
- Per Port: Link, Speed, Activity
- Per Gigabit Port: Link, Speed, Activity, Stack

## **Power Supply**

Power Consumption: 35.1W  
100-240VAC/50-60 Hz universal input

## **Package Contents**

- GS724TS ProSafe 24 port Gigabit Smart Stackable Switch with 4 shared SFP Ports
- Rubber footpads
- Power cord
- One stacking cable
- Rack-mount kit Resource CD Installation Guide
- Warranty/Support information card

## **Administrative Switch Management**

- IEEE 802.1Q VLAN (128 groups, Static)
- IEEE 802.1p Class of Service (CoS)
- Port-based QoS
- IEEE 802.3ad Static or Dynamic Link Aggregation (LACP)
- IEEE 802.1D Spanning Tree Protocol
- SNMP v1, v2c, v3
- RFC 1213 MIB II
- RFC 1643 Ethernet Interface MIB
- RFC 1493 Bridge MIB
- RFC 2131 DHCP client
- IEEE 802.1x (RADIUS)
- Access Control List (ACL)
- Layer 3 (DSCP) Quality of Service (QoS)
- TACACS+
- Port-based security by locked MAC addresses
- Storm control for broadcast, multicast and unknown unicast packets
- Port-based ingress/egress rate limiting
- SNTP
- RMON group 1, 2, 3, 9
- Private Enterprise MIB
- Port Mirroring Support
- Cable test
- Web-based configuration
- Configuration Backup/Restore
- Password Access Control
- Firmware upgradeable

## **Performance Specifications**

- Forwarding modes: Store-and-forward
- Bandwidth: 48 Gbps
- Stacking bandwidth: 20 Gbps
- Network latency: Less than 20 microseconds for 64-byte frames in store-and-forward mode for 1000 Mbps to 1000 Mbps transmission
- Buffer memory: 128 KB
- Address database size: 8,000 media access control (MAC) addresses per system
- Addressing: 48-bit MAC address
- Mean Time Between Failure (MTBF): 100,000 hours (~11 years)

# Anexo II.D

## Punto de acceso inalámbrico (WAP).

# SWITCH NETGEAR 24PTOS 10/100/1000 GB PORT STACKABLE(GS724TS)



**NETGEAR**

## Network Protocol and Standards Compatibility

- IEEE 802.3 10BASE-T
- IEEE 802.3u 100BASE-TX
- IEEE 802.3ab 1000BASE-T
- IEEE 802.3z 1000BASE-X
- IEEE 802.3x full-duplex flow control

## Interfaces

- 24 10/100/1000 Mbps switching ports
- 4 Built-in shared SFP Gigabit Ethernet fiber ports for 100/1000 Mbps connectivity
- Auto-sensing and auto-negotiating capabilities for all copper ports
- Auto Uplink™ on all ports to make the right connection

## Administrative Switch Management

- IEEE 8021.Q VLAN (128 groups, Static)
- IEEE 802.1p Class of Service (CoS)
- Port-based QoS
- IEEE 802.3ad Static or Dynamic Link Aggregation (LACP)
- IEEE 802.1D Spanning Tree Protocol
- SNMP v1, v2c, v3
- RFC 1213 MIB II
- RFC 1643 Ethernet Interface MIB
- RFC 1493 Bridge MIB
- RFC 2131 DHCP client
- IEEE 802.1x (RADIUS)
- Access Control List (ACL)
- Layer 3 (DSCP) Quality of Service (QoS)
- TACACS+
- Port-based security by locked MAC addresses
- Storm control for broadcast, multicast and unknown unicast packets
- Port-based ingress/egress rate limiting
- SNTP
- RMON group 1, 2, 3, 9
- Private Enterprise MIB
- Port Mirroring Support
- Cable test
- Web-based configuration
- Configuration Backup/Restore
- Password Access Control
- Firmware upgradeable

## Performance Specifications

- Forwarding modes: Store-and-forward
- Bandwidth: 48 Gbps
- Stacking bandwidth: 20 Gbps
- Network latency: Less than 20 microseconds for 64-byte frames in store-and-forward mode for 1000 Mbps to 1000 Mbps transmission
- Buffer memory: 128 KB
- Address database size: 8,000 media access control (MAC) addresses per system
- Addressing: 48-bit MAC address
- Mean Time Between Failure (MTBF): 100,000 hours (~11 years)

## LEDs

- Unit: Power, Master, Stack ID
- Per Port: Link, Speed, Activity
- Per Gigabit Port: Link, Speed, Activity, Stack

## Power Supply

Power Consumption: 35.1W  
100-240VAC/50-60 Hz universal input

## Package Contents

- GS724TS ProSafe 24 port Gigabit Smart Stackable Switch with 4 shared SFP Ports
- Rubber footpads
- Power cord
- One stacking cable
- Rack-mount kit Resource CD Installation Guide
- Warranty/Support information card

# Anexo II.E

## Servidor gama media

### Dell™ Poweredge™ 2900

# SERVIDOR DELL POWER EDGE 2900



**Diseñado con características de próxima generación, gran capacidad de memoria y excepcional capacidad de ampliación, el servidor Dell™ PowerEdge™ 2900 es perfecto para la consolidación de aplicaciones de mensajería/collaboración, bases de datos y archivos/impresión tanto en un centro de datos como en oficinas remotas/filiales**

## 9<sup>a</sup> generación de innovadores servidores PowerEdge de Dell

Gracias a un diseño de hardware innovador, a la compatibilidad de software y al continuo enfoque en minimizar las actualizaciones del sistema, la 9<sup>a</sup> generación de servidores PowerEdge de Dell ayuda a reducir la complejidad que implica la administración de datos, tanto si se trata de una empresa grande o pequeña. Estos servidores están diseñados para una Especificación conductual desarrollada por Dell™ que define un formato de hardware y una interacción del usuario uniformes en todos los modelos de esta generación y de futuras generaciones de PowerEdge. Además, una imagen del sistema principal compartida con 1950 y 2950 permite las actualizaciones del BIOS, los drivers del sistema, el firmware, los sistemas operativos y las aplicaciones desde una plantilla fácil de copiar para una administración de software simplificada. Con los últimos procesadores Intel® Xeon®, los servidores de 9<sup>a</sup> generación PowerEdge ofrecen la potencia y el rendimiento que espera de Dell.

## Dell PowerEdge 2900 ofrece un rendimiento a nivel empresarial

El servidor Dell PowerEdge 2900 está diseñado para proporcionar un rendimiento excelente en un chasis de torre o una opción con posibilidad de montaje en rack de 5U con procesadores de cuatro núcleos de próxima generación Intel Xeon, tecnología de memoria DIMM con memoria intermedia completa y unidades de disco duro SCSI conectadas de serie. También admite doce ranuras de memoria para 48 GB de capacidad para cargas de trabajo y aplicaciones que utilizan la memoria de forma intensiva. Y la funcionalidad del motor de carga TCP/IP en la tarjeta NIC Gigabit integrada ayuda a optimizar el rendimiento y el uso de la CPU moviendo el procesamiento del protocolo TCP/IP a la NIC.

## Flexibilidad y capacidad de ampliación para entornos en crecimiento

El servidor Dell PowerEdge 2900 se ha fabricado teniendo en cuenta la flexibilidad. Ofrece la variedad más amplia de opciones de configuración disponibles en un servidor Dell de dos zócalos. Puede escoger entre opciones de chasis de torre o rack con unidades de disco duro SAS o SATA conectables en marcha y entre distintos dispositivos ópticos y productos en cinta para un almacenamiento interno de hasta 3.0 TB. Además, el sistema incluye seis ranuras de E/S. Y debido a que la Tarjeta de acceso remoto Dell (DRAC) y el driver PERC 5/i integrado utilizan ranuras de tarjetas secundarias, es posible ampliar cada una de las seis ranuras de E/S. Tiene la opción de añadir hasta cuatro tarjetas de interfaz de red (NIC) Gigabit y dos dispositivos de almacenamiento de canal dual para proporcionar un potencial de crecimiento increíble.



Dell PowerEdge 2900

## Disponibilidad fiable para maximizar el tiempo de actividad

Con características de alta disponibilidad tales como las unidades de disco duro conectables en marcha y las fuentes de alimentación/ventiladores redundantes, Dell PowerEdge 2900 ayuda a preservar la fiabilidad de los datos que se mueven en su organización. También proporciona asistencia para distintas opciones de RAID incluido el RAID integrado con 256 MB de caché con reserva de memoria por batería para que se pueda acceder a su información más valiosa de forma fiable.

## Facilidad de administración para una complejidad reducida

El servidor Dell PowerEdge 2900 está equipado con un Driver de administración de la placa base (BMC) que incluye un conjunto de herramientas completo que supervisa el hardware de servidor, le avisa cuando se producen fallos en el servidor y permite las operaciones remotas básicas. Para entornos con servidores ubicados en centros de datos seguros o en sitios que carecen de personal de TI, Dell ofrece una característica opcional para los servidores PowerEdge, el Driver de acceso remoto de Dell (DRAC). Funciona mediante una interfaz de usuario gráfica basada en, DRAC puede admitir la supervisión, la solución de problemas, la reparación, las actualizaciones y el acceso remoto del estado del sistema operativo. Un software común con la misma familia de servidores de 9<sup>a</sup> generación PowerEdge ayudan a simplificar aún más la administración. Además, la Especificación conductual de Dell proporciona una plataforma conocida para una facilitan la implementación, la administración y los servicios e implica una reducción del coste total de la propiedad (TCO) en diversas generaciones de servidores PowerEdge.





# SERVIDOR DELL POWEREDGE 2900

## SERVICIOS DE INFRAESTRUCTURA DE TI DE DELL

Dell aporta ejecución pura a los Servicios de TI. La planificación, implementación y mantenimiento de su infraestructura de TI no merece menos. La variabilidad en la ejecución puede afectar a la productividad del usuario, los recursos de TI y, en definitiva, a su reputación. Al aprovechar nuestra herencia en la calidad de dirección del proceso, en Dell Services podemos ofrecer un método más inteligente.

No pretendemos hacerlo todo. Nos centramos en los servicios de infraestructura de TI. Y tomamos un enfoque dirigido hacia el cliente, basándonos en la filosofía de que usted conoce su negocio mejor que nadie. Por eso Dell no intenta tomar decisiones clave sin su conocimiento o le ofrece más de lo que necesita. Todo lo contrario, aplicamos nuestra administración de procesos a nivel mundial y nuestra cultura "sin excusas" para ofrecer lo que nuestros clientes necesitan más actualmente: flexibilidad y calidad constante. Esto es pura ejecución. Esto es Dell en estado puro.

### Servicios de evaluación, diseño e implementación

Los departamentos de TI continuamente se enfrentan al reto de evaluar e implementar nuevas tecnologías. Los servicios de evaluación, diseño e implementación de Dell pueden reestructurar su entorno de TI para mejorar el rendimiento, escalabilidad y eficacia al tiempo que contribuyen a maximizar su inversión y minimizar la interrupción de su negocio.

### Servicios de implementación

La implementación del sistema es un mal necesario que invade casi todas las organizaciones. Debe implementar nuevos sistemas para ayudar a mejorar el rendimiento y satisfacer los requisitos del usuario. Con los servicios de implementación de Dell, ayudamos a simplificar y acelerar la implementación y el uso de nuevos sistemas para maximizar el tiempo de actividad en su entorno de TI.

### Recuperación y reciclado de activos

La eliminación, reventa y donación correctas del equipo informático constituyen una larga tarea que suele encontrarse al final de muchas listas de tareas informáticas. Dell simplifica los procesos de caducidad del equipo informático de modo que maximiza el valor para los clientes.

### Servicios de formación

Aporte a sus empleados los conocimientos y habilidades que necesiten para ser tan productivos como sea posible. Dell ofrece extensos servicios de formación que incluyen formación en hardware y software, así como clases de desarrollo profesional. Con la formación de Dell, puede contribuir a mejorar la fiabilidad del sistema, maximizar la productividad y reducir las peticiones del usuario final y el tiempo de inactividad.

### Servicios de asistencia técnica a empresas

Con Dell, puede obtener el máximo rendimiento y disponibilidad de su servidor y sistemas de almacenamiento Dell. Los Servicios de asistencia de nuestra empresa ofrecen un mantenimiento proactivo para ayudar a evitar problemas y para responder y solucionar rápidamente los problemas cuando se produzcan. Hemos construido una infraestructura global que ofrece distintos niveles de asistencia empresarial para los sistemas de su infraestructura.

Para ayudarle a obtener el máximo provecho de sus sistemas Dell, visite [www.dell.com/services](http://www.dell.com/services).

Los servicios varían según la zona.

## CARACTERÍSTICAS SERVIDOR DELL™ POWEREDGE™ 2900

<b>Formato</b>	Torre o montaje en rack de 5U
<b>Procesadores</b>	Hasta dos procesadores de secuencia de doble núcleo Intel® Xeon® 5000 con 3.0 GHz de frecuencia de reloj o hasta dos procesadores de secuencia de doble núcleo Intel Xeon 5100 con 3.0 GHz de frecuencia de reloj o hasta dos procesadores de secuencia de cuatro núcleos Intel Xeon 5300 con 2,66 GHz de frecuencia de reloj
<b>Bus frontal</b>	Secuencia 5000: 667 MHz o 1066 MHz Secuencia 5100: 1066 MHz o 1333 MHz Secuencia 5300: 1066 MHz o 1333 MHz
<b>Caché</b>	Secuencia 5000: caché de nivel 2 de 2 MB por procesador Secuencia 5100: caché de nivel 2 de 4 MB por procesador Secuencia 5300: caché de nivel 2 de 2 x 4 MB por procesador.
<b>Conjunto de chips</b>	Intel 5000X
<b>Memoria</b>	Módulos DIMM de 256 MB/512 MB/1 GB/2 GB/4 GB con memoria intermedia completa (FBD) en pares coincidentes; 533 MHz o 667 MHz; 12 zócalos para DIMM FBD para admitir hasta 48 GB
<b>Canales de E/S</b>	Seis en total: Dos ranuras x 133 MHz PCI-X® en un solo bus PCI; una ranura x8 PCI Express®; tres ranuras x4 PCI Express; 2 NIC Gigabit integradas; puerto de administración para DRAC5
<b>Drivers integrados</b>	PERC 5/i (opcional); driver RAID SAS 3 Gb/s RAID con procesador Intel IOP333 y caché de 256 MB; SAS 5/i (base); driver SAS de 4 puertos con procesador ARM966 (no admite RAID)
<b>Driver RAID complementario</b>	PERC 4e/DC opcional (driver RAID PCI Express de canal dual); Adaptador PERC 5/E opcional para almacenamiento RAID externo
<b>Compartimentos de disco duro</b>	Compartimentos internos de unidad de disco duro estándar que admiten hasta ocho unidades de disco duro SAS o SATA de 3,5" conectables en marcha; Flexbay que admite hasta dos unidades de 3,5" conectables en marcha o dispositivo de cinta de altura completa; compartimento periférico que admite dos dispositivos de altura media (unidad de cinta más una unidad de CD-ROM opcional, DVD-ROM opcional o una unidad combinada de CD-RW/DVD-ROM); compartimento para unidad de disquete de 3,5" opcional
<b>Almacenamiento interno máximo</b>	Hasta 3 TB <sup>1</sup>
<b>Discos duros<sup>2</sup></b>	Unidades de disco duro SAS de 3,5" (a 10.000 rpm) de 73 GB, 146 GB o 300 GB conectables en marcha; unidades de disco duro SAS de 3,5" (a 15.000 rpm) de 36 GB, 73 GB o 146 GB conectables en marcha; unidades de disco duro SATA de 3,5" (a 7.200 rpm) de 80 GB, 160 GB o 250 GB conectables en marcha <sup>3</sup>
<b>Almacenamiento interno</b>	10 unidades SAS de 3,5" conectables en marcha (a 10.000 y 15.000 rpm) o 10 unidades SATA a 7.200 rpm
<b>Almacenamiento externo</b>	Dell PowerVault™ 22xS SCSI, PowerVault MD1000, productos Dell/EMC
<b>Opciones de copia de seguridad en cinta</b>	Internas: PowerVault 100T y 110T Externas: PowerVault 114T, 122T, 124T, 132T, 136T, 160T y ML6000
<b>Tarjeta de interfaz de red</b>	NIC Gigabit Ethernet Broadcom® NetXtreme II™ 5708 dual integrada <sup>4</sup> NIC Ethernet con compensación de carga y capacidad de recuperación. TOE (motor de carga TCP/IP) compatible con Microsoft Windows Server 2003, SP1 o superior con Scalable Networking Pack. Tarjetas NIC complementarias opcionales: Adaptador de servidor de puerto dual Intel® PRO/1000 PT, Gigabit, Copper, PCI-E x4; adaptador de servidor de un solo puerto Intel® PRO/1000 PT, Gigabit, Copper, PCI-E x1; adaptador de servidor de un solo puerto Intel® PRO/1000 PF, Gigabit, óptico, PCI-E x4; NIC Gigabit Ethernet de un solo puerto Broadcom® NetXtreme™ 5721, Copper, PCI-E x1; NIC Gigabit Ethernet de un solo puerto Broadcom® NetXtreme II™ 5708 con TOE, Copper, PCI-E x4
<b>Módem</b>	Módem interno Conexant V.92 opcional
<b>Fuente de alimentación</b>	Fuente de alimentación redundante opcional de 930 vatios conectable en marcha
<b>Disponibilidad</b>	Unidades de disco duro conectables en marcha, fuente de alimentación redundante opcional conectable en marcha, refrigeración redundante, memoria ECC, banco de reserva; Single Device Data Correction (SDDC); tarjeta secundaria PERC 5/i integrada con caché con reserva de memoria por batería; soporte de comutación por error de alta disponibilidad; DRAC5; chasis sin necesidad de herramientas; compatibilidad con clústeres
<b>Vídeo</b>	ATI ES1000 integrada con memoria de 16 MB
<b>Administración remota</b>	Driver de administración de la placa base estándar compatible con IMPI 2.0; DRAC5 opcional para funciones avanzadas
<b>Administración de sistemas</b>	OpenManage™
<b>Compatibilidad con rack</b>	4 postes (rack Dell), 2 postes y guías Versa de terceros, guías móviles y brazo para la manipulación de cables
<b>Sistemas operativos</b>	Microsoft® Windows® Server 2003 R2, Standard, Enterprise Edition, x64, Standard y Enterprise Edition; Microsoft® Windows® Server 2003 Small Business Standard, Premium Edition; Microsoft® Windows® Storage Server 2003 R2, Standard, Enterprise Edition; Red Hat® Linux® Enterprise v4, ES EM64T; SUSE Linux Enterprise Server 9 EM64T, SP3

<sup>1</sup> Soporte de disco duro SATA de 250 GB en Q3CY06.

<sup>2</sup> Para las unidades de disco duro, GB significa 1.000.000.000 de bytes; la capacidad total accesible varía en función del material preconfigurado y el entorno operativo y será inferior.

<sup>3</sup> Este término no conlleva una velocidad de funcionamiento real de 1 GB/seg. Para la transmisión de alta velocidad se necesita una conexión a un servidor Gigabit Ethernet e infraestructura de red.

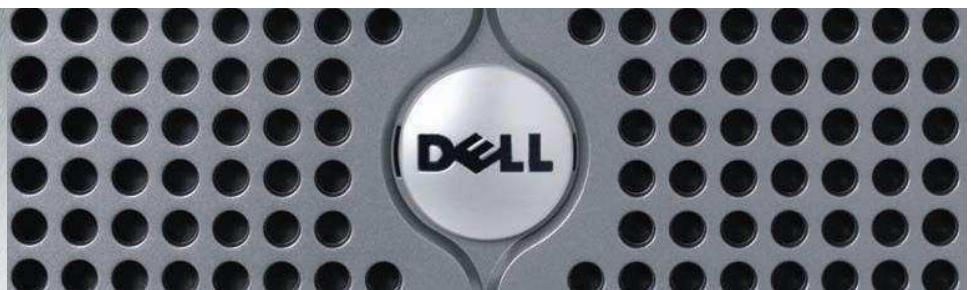
Dell no se hace responsable de ningún error tipográfico ni fotográfico. Dell, el logotipo de Dell y PowerEdge son marcas comerciales de Dell Inc. Intel y Xeon son marcas comerciales registradas de Intel Corporation. PCI Express es una marca comercial y PCI-X es una marca comercial registrada de PCI-SIG. El resto de marcas registradas y nombres comerciales se pueden usar en este documento para hacer referencia a entidades que reclaman las marcas, los nombres o sus productos. Dell renuncia a cualquier interés en la propiedad de las marcas y los nombres de terceros. © Copyright 2006 Dell Inc. Todos los derechos reservados. Queda totalmente prohibida cualquier tipo de reproducción sin el permiso por escrito de Dell Inc. Para obtener más información, póngase en contacto con Dell, Mayo de 2006.

# Anexo II.F

## Servidor gama baja

### Dell™ Poweredge™ 840.

## SERVIDOR DELL POWEREDGE 840



**Ideal para oficinas remotas y pequeñas empresas, el servidor™ PowerEdge™ 840 de Dell ofrece características avanzadas a un precio asequible.**

### Rendimiento flexible

Tanto si se trata de una empresa pequeña, una compañía con varias localizaciones o una organización grande con oficinas remotas, tiene unas necesidades exclusivas. El servidor PowerEdge 840 de Dell le da una opción de potencia de procesamiento de manera que su servidor pueda ofrecerle lo que necesita.

Para lograr un rendimiento óptimo y varias aplicaciones, PowerEdge 840 admite los procesadores de secuencia Dual-Core Intel® Xeon® 3000 con la nueva tecnología de doble núcleo que combina dos unidades de procesamiento en un único chip de procesador. Es un servidor de propósitos generales para aplicaciones de grupos de trabajo pequeños como la mensajería y el acceso a Internet y la Web al servicio de los empleados. La potencia de procesamiento de doble núcleo tiene como resultado el aumento significativo del rendimiento y la eficacia del sistema de alimentación en comparación con los procesadores de un solo núcleo.

Si necesita un rendimiento excepcional al mejor precio, el Intel Pentium® D es perfecto para entornos de una sola aplicación. Para realizar las tareas de archivo e impresión, el servidor PowerEdge 840 equipado con un procesador Celeron® D le proporciona la solución adecuada para su organización.

### Fiabilidad y disponibilidad

Lograr el mejor rendimiento de su servidor es una parte importante de una solución económica. El servidor PowerEdge 840 está diseñado para garantizar el máximo tiempo de actividad y la protección de los datos. Las unidades de disco duro de acceso frontal SAS o SATA que facilitan el cambio de unidad con el menor tiempo de inactividad son una característica especialmente recomendable para los entornos de punto de ventas que necesiten actualizar las bases de datos de precios. Además, las matrices RAID SAS/SATA permiten continuar utilizando el servidor aunque falle una unidad.

Por otra parte, el servidor PowerEdge 840 es compatible con las soluciones de copia de seguridad en cinta de gran capacidad y almacenamiento externo para una protección y disponibilidad de datos fiables. Puede admitir las unidades de copia de seguridad en cinta interna IDE o SCSI, cinta externa SCSI y soluciones de almacenamiento de acceso directo.

### Facilidad de administración local y remota

La administración de servidores a grandes distancias puede comprometer la eficacia y rentabilidad en general. El servidor PowerEdge 840 está específicamente diseñado para proporcionar a los administradores de TI funciones de administración local y remota excepcionales. El servidor viene equipado con completas herramientas de administración que ayudan a reducir el mantenimiento y los costes de propiedad.

Dell Server Assistant proporciona una configuración, instalación del sistema operativo y funciones de configuración sencillos mientras que Dell OpenManage™ IT Assistant Suite ayuda a garantizar una administración sencilla durante la vida de su servidor. La Tarjeta de acceso remoto de Dell (DRAC) hace más fácil que nunca el acceso, la supervisión y la solución de problemas.

Céntrese en llevar su empresa adelante en lugar de en su servidor y deje que Dell haga el trabajo en su lugar. Los servicios de Dell le ofrecen sistemas operativos preinstalados, Integración de fábrica personalizada para hardware y software preconfigurado y Servicio de instalación del servidor a domicilio.

El servidor PowerEdge 840 ofrece a las pequeñas empresas y a las oficinas remotas una solución flexible, asequible, fiable y fácil de administrar.



Dell PowerEdge 840





# SERVIDOR DELL POWEREDGE 840

## SERVICIOS DE INFRAESTRUCTURA DE TI DE DELL

Dell aporta ejecución pura a los Servicios de TI. La planificación, implementación y mantenimiento de su infraestructura de TI no merece menos. La variabilidad en la ejecución puede afectar la productividad del usuario, los recursos de TI y, en definitiva, a su reputación. Al aprovechar nuestra herencia en la calidad de dirección del proceso, en Dell Services podemos ofrecer un método más inteligente.

No pretendemos hacerlo todo. Nos centramos en los servicios de infraestructura de TI. Y tomamos un enfoque dirigido hacia el cliente, basándonos en la filosofía que usted conoce su negocio mejor que nadie. Por eso Dell no intenta tomar decisiones claves en su conocimiento o le ofrece más de lo que necesita. Todo lo contrario, aplicamos nuestra administración de procesos a nivel mundial y nuestra cultura "sin excusas" para ofrecer lo que nuestros clientes necesitan más actualmente: flexibilidad y calidad constante. Eso es absoluta ejecución. Eso es Dell.

### Servicios de evaluación, diseño e implementación

Los departamentos TI están continuamente renovándose para evaluar e implementar nuevas tecnologías. Los servicios de evaluación, diseño e implementación de Dell pueden reestructurar su entorno de TI para mejorar el rendimiento, escalabilidad y eficacia al tiempo que contribuyen a maximizar su inversión y minimizar la interrupción de su negocio.

### Servicios de implementación

La implementación del sistema es un mal necesario que invade casi todas las organizaciones. Deberá implementar sistemas nuevos que le ayuden a mejorar el rendimiento y a adaptarse a las demandas del usuario. Con los servicios de implementación de Dell, ayudamos a simplificar y acelerar la implementación y el uso de nuevos sistemas para maximizar el tiempo de actividad en su entorno de TI.

### Recuperación y reciclado de activos

La eliminación, reventa y donación correctas del equipo informático constituyen una larga tarea que suele encontrarse al final de muchas listas de tareas informáticas. Dell simplifica los procesos de caducidad del equipo informático de modo que maximiza el valor para los clientes.

### Servicios de formación

Aporte a sus empleados los conocimientos y habilidades que necesiten para ser tan productivos como sea posible. Dell ofrece extensos servicios de formación que incluyen formación en hardware y software, así como clases de desarrollo profesional. Con la formación de Dell, puede contribuir a mejorar la fiabilidad del sistema, maximizar la productividad y reducir las peticiones del usuario final y el tiempo de inactividad.

### Servicios de asistencia técnica a empresas

Con Dell, puede obtener el máximo rendimiento y disponibilidad de su servidor y sistemas de almacenamiento Dell. Los Servicios de asistencia de nuestra empresa ofrecen un mantenimiento proactivo para ayudar a evitar problemas y para responder y solucionar rápidamente los problemas cuando se produzcan. Hemos construido una infraestructura global que ofrece distintos niveles de asistencia para los sistemas de su infraestructura.

Para sacar el mejor partido de sus sistemas Dell, visite [www.dell.com/services](http://www.dell.com/services).

Los servicios varían según la región.

[www.dell.com](http://www.dell.com)

## CARACTERÍSTICAS SERVIDOR™ POWEREDGE™ 840 DE DELL

<b>Formato</b>	Sólo torre
<b>Procesadores</b>	Procesador de secuencia de un solo núcleo Intel® Xeon® 3000 de hasta 2,66 GHz; Procesador de un solo núcleo Intel Pentium® D de 2,8 GHz; un procesador Intel Celeron® D de 2,8 GHz
<b>Bus frontal</b>	1066 MHz del Intel Xeon de secuencia 3000; 800 MHz del Intel Pentium D; 533 MHz del Intel Celeron D
<b>Caché</b>	Hasta 4 MB de caché de segundo nivel para el Intel Xeon de secuencia 3000; 2x2 MB de caché de segundo nivel para el Intel Pentium D; 256 K de caché de segundo nivel para el Intel Celeron D
<b>Conjunto de chips</b>	Intel 3000
<b>Memoria</b>	Memoria SDRAM de 512 MB-8 GB con ECC y DDR-2 533/667
<b>Ranuras de E/S</b>	Cinco en total: dos ranuras PCI Express™ (canal 1x8 y canal 1x1); dos ranuras PCI-X® (de 64 bits a 133 MHz y 3,3 V); una ranura PCI (de 32 bits a 33 MHz)
<b>Controlador de la unidad</b>	SATA integrado; SAS opcional
<b>Controlador RAID</b>	SAS 5i/R, PERC 5/i con batería, PERC 5/e
<b>Compartimentos de disco duro</b>	4 SATA o SAS conectables en marcha/de acceso frontal o con cableado de 3,5" 1 CD, CD/DVD-ROM, combinado de CD-RW/DVD opcionales de 5,25" 1 TBU interna opcional de media altura de 5,25" 1 unidad de disquete de 3,5"
<b>Almacenamiento interno máximo</b>	Hasta 1,2 TB: cuatro SAS conectables en marcha o con cableado de 300 GB (a 10.000 rpm); Hasta 584 GB: cuatro SAS conectables en marcha o con cableado de 146 GB (a 15.000 rpm); Hasta 2 TB: cuatro SATA conectables en marcha o con cableado de 500 GB (a 7.200 rpm);
<b>Discos duros<sup>1</sup></b>	SAS de 3,5" (10.000 rpm): 73 GB, 146 GB, 300 GB; SAS de 3,5" (a 15.000 rpm): 36 GB, 73 GB, 146 GB; SATA de 3,5" (a 7.200 rpm): 80 GB, 160 GB, 250 GB, 500 GB
<b>Almacenamiento externo</b>	PowerVault™ MD1000
<b>Opciones de copia de seguridad en cinta</b>	TR40 (IDE) y DAT72(SCSI)
<b>Tarjeta de interfaz de red</b>	Una tarjeta NIC Broadcom Gigabit <sup>2</sup> integrada; Una tarjeta opcional NIC Intel x4 PCIe Gigabit <sup>2</sup> de doble puerto; Una tarjeta opcional NIC Intel PCIe Gigabit <sup>2</sup> de doble puerto; Broadcom x1 PCIe Gigabit <sup>2</sup> Opcional; NIC con TOE Broadcom x4 PCIe Gigabit <sup>2</sup> opcional
<b>Fuente de alimentación</b>	420 W
<b>Disponibilidad</b>	Memoria con ECC y DDR2-533/667; SAS o SATA conectables en marcha
<b>Vídeo</b>	ATI ES1000 integrada con memoria de 16 MB
<b>Administración remota</b>	Compatibilidad estándar del BMC con la IPMI 1.5; DRAC 4/p opcional para funciones avanzadas
<b>Administración de sistemas</b>	Dell OpenManage™
<b>Compatibilidad con bastidor</b>	Sólo terceros
<b>Sistemas operativos</b>	Microsoft Windows® Storage Server 2003 R2 (x64), versiones Express y Workgroup; Windows 2003 SBS Standard y Premium; Red Hat® Enterprise Linux® ES v3, v4 IA32, v4 para EM64T; SUSE® Linux ES9 EM64T; SUSE® Linux ES10 EM64T

<sup>1</sup> Para las unidades de disco duro, GB significa mil millones de bytes y TB un trillón de bytes; la capacidad actual varía en función del material preconfigurado y el entorno operativo y será inferior.

<sup>2</sup> Este término no conlleva una velocidad de funcionamiento real de 1 GB/seg. Para la transmisión de alta velocidad se necesita una conexión a un servidor Gigabit Ethernet e infraestructura de red.

Dell no es responsable de los errores tipográficos o en las fotografías. Dell, el logotipo de Dell, PowerEdge, PowerVault y OpenManage son marcas comerciales de Dell Inc. Intel, Pentium, Xeon y Celeron son marcas registradas de Intel Corporation. Linux es una marca comercial registrada de Linus Torvalds. Microsoft y Windows son marcas registradas de Microsoft Corporation. Novell y NetWare son marcas comerciales registradas de Novell, Inc. PCI Express es una marca comercial y PCI-X es una marca comercial registrada de PCI-SIG. Red Hat es una marca comercial registrada de Red Hat, Inc. SuSE es una marca comercial de SuSE AG. En este documento se pueden utilizar otras marcas y nombres comerciales para hacer referencia a entidades que están reclamando las marcas y los nombres de sus productos. Dell renuncia a cualquier interés en la propiedad de las marcas y los nombres de terceros. © Copyright 2006 Dell Inc. Todos los derechos reservados. Queda totalmente prohibida cualquier tipo de reproducción sin el permiso por escrito de Dell Inc. Para obtener más información, póngase en contacto con Dell. Agosto de 2006, Kolar.



# Anexo II.G

Componentes del servidor propuesto para servicios de almacenamiento y salva.

# Enlight EN-8950 File Server Case

<b>Product ID</b>	12896
<b>Brand</b>	Enlight
<b>Vendor Code</b>	EN-8950(NO-PSU)
<b>Description</b>	EN-8950
# Intel certifed	
# The optional hot-swap drive module houses five SCA	
# Patented two-way opening front door for convenient use with modularized design	
# Modularized design for easy upgrade and expansion	
# Various modules are available for customers convenience	
# Special Rack can be chosen for CD-Rom when placed in a 19" rail mount	
Specification	
Form Factor	5U Rackmount/Pedestal
Main Board Size	EEB 12" x 13" / ATX 12" x 9.6" / CEB 12" x 10.5"
HDD Bays	
Optional	8702 or 8721
Hot-swap drive module	
Drive Bays	1 x 3.5" drive bay, 9 x 5.25" drive bays
Back Plane	None
Expansion Slot	7 PCI slots
Cooling Fan	2x80 mm rear ball-bearing fans or 1x120mm
LED Indicators	1x PSW, 1x Fan, 1x HDD busy, 1x ERR, 1x Alarm, 1x HDD status, 1x LAN, 3x PSW Status (Redundant PS)
Switch	1 x Power, 1 x Reset
Power Supply	Single 560W / 600W
Redundant	560W / 600W
Dimensions(W x H x D)	480 x 220 x 650 mm
Packing Details	Qty/20' container : 160 pcs
Qty/40' container	: 350 pcs
Qty/40' HQ container	: 400 pcs
Security	2 x Mechanical Lock (Front Bezel)
Padlock Loop	(back panel)
Intrusion Detector	2 x (Front panel & Rear panel)

## ASUS CUV4X-DLS Motherboard



<b>Processor Support</b>	2 Socket 370 for Pentium III Coppermine Processors Feature Setting DIP Switches
<b>Chipsets</b>	VIA VT82C694XDP System Controller VIA VT82C686B PCIset 2Mbit Programmable Flash EEPROM
<b>Main Memory</b>	Maximum 4GB support 4 DIMM Sockets PC133 SDRAM support
<b>Expansion Slots</b>	5 PCI Slots 1 Accelerated Graphics Port (AGP) Pro/4X Slot
<b>System I/O</b>	1 Floppy Disk Drive Connector 2 IDE Connectors (UltraDMA/100 Support) 1 ASUS iPanel Connector 1 Parallel Port 2 Serial Ports (COM1/COM2) LAN Connector (RJ-45) USB Connectors (Port 0 & Port 1) USB Connectors (Port 2 & Port 3) 1 PS/2 Mouse Connector 1 PS/2 Keyboard Connector
<b>Network Features</b>	Intel 82559 Fast Ethernet Controller Wake-On-LAN Connector Wake-On-Ring Connector
<b>Hardware Monitoring</b>	System Voltage Monitoring (integrated in ASUS ASIC) 4 Fan Power and Speed Monitoring Connectors
<b>Special Features</b>	LSI 32-bit (33MHz) Ultra160 SCSI Controller Onboard SCSI Connectors Onboard LED
<b>Audio Features</b>	(on audio models only) AC '97 v2.1 Audio Codec 1 Game/MIDI Port 1 Line Out Connector 1 Line In Connector 1 Microphone Connector
<b>Power</b>	Auxiliary Power Connector ATX Power Supply Connector
<b>Form Factor</b>	ATX