Capítulo 1

Introducción y objetivos

En la actualidad, cada día un mayor número de redes de pequeñas, medianas o grandes empresas que prestan servicios a través de Internet o que necesitan tomar servicios desde Internet establecen sistemas cortafuegos o *firewalls* para proteger sus sistemas de posibles ataques e intrusiones desde el exterior. Desde la simple configuración adecuada de los *routers* que les conectan a la *World Wide Web* hasta la instalación de complejas zonas desmilitarizadas o *DMZs*, dichos usuarios confían en el éxito que tendrán sus políticas de seguridad y en su funcionamiento autónomo y automatizado para despreocuparse, hasta cierto punto, del estado de su red.

Sin embargo esta despreocupación puede ser falsamente provocada: según el Instituto Nacional de Estadística durante el año 2003/2004 un 33,8 % de las empresas españolas declararon haber tenido algún problema de seguridad informática, mientras que la cifra durante el año 2004/2005 se redujo a un 27,3 %. Si sumamos a esta información que más del 90 % de las empresas españolas de más de diez empleados dispone de un acceso a Internet, cabe pensar que realmente el problema no da lugar a la citada despreocupación.

En los *firewalls* se implementan muchas funciones de control y sus configuraciones pueden ser de una cierta madurez y complejidad. Existe, por tanto, una necesidad creciente de *monitorizar* el estado de los sistemas *firewall* así como el uso de los recursos de la red de área local, y esta monitorización no debe servir únicamente para realizar una gestión de la contabilidad sino que debe usarse también como un agente de prevención de ataques externos o internos. Por lo tanto, de las cinco áreas funcionales de gestión definidas en el modelo OSI, este Proyecto se enmarca dentro de las áreas de Gestión de la Seguridad y de la Gestión de Contabilidad.

Como podemos intuir, las topologías de las redes o de los sistemas de cortafuegos que establezcan en las empresas son muy variables y pueden tener estructuras muy distintas. Las preguntas a las que trataremos de responder a lo largo de este Proyecto intentan no centrarse sobre ninguna estructura específica, sino que abordan distintos aspectos que ilustraremos con un ejemplo genérico:

> Si administramos una red grande de una empresa corporativa con distintas subredes para distintos departamentos cada una de ellos con sus propios *firewalls*, distintas *DMZs* para distintos accesos a Internet, ¿cómo monitorizar las distintas subredes? ¿Cómo analizar las necesidades de tráfico y ancho de banda de los departamentos? ¿Cómo comprobar el estado o las alarmas de los distintos *firewalls* y sistemas alojados en distintos segmentos de la red? ¿Cómo centralizar esa información? ¿Cómo hacerlo de forma eficiente?

Estas son las distintas preguntas a las que vamos a intentar dar respuesta en este Proyecto de Fin de Carrera.

La falta de herramientas de *software* libre que solucionen los problemas anteriomente mencionados motiva la realización de este Proyecto de Fin de Carrera. Por lo tanto, el objetivo de este Proyecto es la creación de un sistema de monitorización remota que cumpla las siguientes necesidades:

- Será un sistema de monitorización remota, en el que la información de monitorización será generada en los sistemas remotos y enviada a otros sistemas para su almacenamiento y procesado.
- Será un sistema centralizado.
- Será un sistema escalable y adaptable al tamaño de la red que se desee monitorizar.
- Será un sistema que en *software* se basará en **GNU/Linux**.

El resto del presente documento de este Proyecto de Fin de Carrera se estructura en los siguientes capítulos autocontenidos:

Primero, en el capítulo 2, "*Análisis de requisitos y descripción funcional del sistema*", haremos una reflexión acerca de este Proyecto, realizando un análisis más detallado de la problemática a solventar y haciendo una aproximación al sistema que se pretende desarrollar.

Tras ello, en el capítulo 3, "*Planificación y costes*", planteamos la planificación y evaluación de costes estimadas para el desarrollo de este Proyecto.

En el capítulo 4, "*Monitorización estadística de tráfico*", hablaremos sobre la recogida de información estadística del tráfico de la red, apoyándonos para ello en el protocolo *NetFlow*.

En el capítulo 5, "*Monitorización de tráfico*", veremos las posibilidades de recogida de información completa de tráfico desde un sistema remoto, haciendo uso de configuraciones específicas de *iptables*.

En el capítulo 6, "*Recogida de registros*", hablaremos sobre la recogida de registros, de informes de incidencias y de estado de las máquinas que dan soporte a nuestra red, basándonos para ello en *syslog-ng*.

Tras ello, en el capítulo 7, "*Tratamiento de la información*", veremos algunas posibilidades para la visualización y manejo de la información de gestión recogida con las utilidades anteriores.

En el capítulo 8, "*Interfaz de configuración*", trataremos algunos aspectos acerca de la interfaz de configuración de las utilidades seleccionadas desarrollada en este Proyecto.

Finalmente, en los apéndices del documento se tratarán, entre otros, aspectos de instalaciones y configuraciones de las utilidades empleadas, así como aspectos del desarrollo de la interfaz.