Apéndice F

Validación y pruebas realizadas

F.1. Escenario de pruebas

Para la comprobación del correcto funcionamiento de las utilidades seleccionadas así como de la interfaz que las maneja se dispuso de un entorno de pruebas. Durante esta sección se verán los distintos pasos necesarios para replicar dicho entorno:

1. Disposición de una instalación del sistema operativo **Debian Sarge** funcional y limpia. No se ha tratado en este documento la instalación de dicho sistema operativo pues no se considera que sea materia propia del Proyecto. Sin embargo, sí señalamos los siguientes puntos:

   a) La máquina sobre la que se instale deberá disponer al menos de una tarjeta de red. En nuestro caso se dispuso de una tarjeta de red *ethernet* a la que se dió la dirección IP 192.168.100.24.

   b) La instalación del sistema operativo **Debian Sarge** no necesitará en ningún caso de un entorno gráfico, si bien en el entorno de pruebas utilizado sí se disponia del mismo al ser utilizado el propio sistema de pruebas como sistema de escritorio.

2. Instalación en el sistema **Debian Sarge** de la sonda *fprobe-ng*. La sonda se configuró para su funcionamiento en modo promiscuo en la interfaz con dirección IP 192.168.100.24, y la información recogida por la misma se envió a la dirección IP 192.168.100.24 y concretamente al puerto UDP 555 a través de *NetFlow* versión 7 (aunque posteriormente se cambió, por motivos de testado, a versión 5).

   Con esta configuración ya adelantamos que la sonda y el recolector de *NetFlow* estarán instalados sobre un mismo sistema.

   Más detalles sobre la instalación y configuración de la sonda pueden consultarse en el apéndice A.2, "*Instalación y configuración de la sonda*".

3. Instalación en el sistema **Debian Sarge** del recolector *flow-capture*. No será necesario hacer ningún tipo de configuración adicional en el recolector

ya que es uno de los objetivos de las pruebas comprobar la configuración existente a través de la interfaz de configuración y darle la configuración adecuada para recibir la información de *NetFlow* generada por la sonda instalada en el punto anterior.

Más detalles sobre la instalación del recolector *flow-capture* pueden verse en el apéndice A.3.1, "*Instalación de flow-tools*".

4. Instalación en el sistema **Debian Sarge** del analizador *FlowScan* y sus módulos *CUFlow* y *CUGrapher*. Además será necesario realizar la configuración manual de algunos parámetros no manejados por la interfaz de configuración, parámetros no ligados directamente al uso de la aplicación sino a su funcionamiento interno y presentación. Esos parámetros serán:

   a) Modificar la directiva `ReportClasses` de *FlowScan* para que haga uso del módulo `CUFlow`.

   b) Crear y ubicar la *script* para el manejo del servicio de *FlowScan*, ubicándola en la ruta adecuada.

   c) Modificar las directivas `OutputDir`, `Scoreboard` y `AggregateScore` de *CUFlow* para que realicen el almacenamiento de sus archivos (no donde ubicarán sus salidas) en directorios válidos del sistema.

   d) Modificar la directiva `OutputDir` de la configuración de *CUGrapher* para que coincida con el valor que contiene la misma directiva de la configuración de *CUFlow*.

   e) Si se desea, modificar las directivas adicionales para una configuración más ajustada de *CUGrapher*.

   No se realizarán más cambios en las configuraciones de *FlowScan* o *CUFlow* dado que es objetivo de la interfaz la modificación de las mismas.

   Se puede consultar más información acerca de este proceso de instalación y las configuraciones pertinentes a lo largo del apéndice D.1.4, "*Exportando a bases de datos Round Robin*".

5. Instalación en el sistema **Debian Sarge** del servidor *Web lighttpd*. Dicho servidor será configurado para atender peticiones en la dirección IP 192.168.100.24, de manera que nuestro sistema centralizado de monitorización, y concretamente la interfaz de coniguración, será accesible en dicha dirección IP.

   Detalles sobre la instalación del servidor *lighttpd* y su adecuada configuración se muestran en el apéndice E.1.1, "*Servidor Web: lighttpd*".

6. Dotar al servidor *Web lighttpd* de soporte para PHP. Para ello será necesaria la instalación de *PEAR* en el sistema **Debian Sarge**.

   Puede leerse más acerca de la instalación y configuración del soporte PHP en el apéndice E.1.2, "*Soporte PHP: PEAR*".

7. Proceder a la instalación de la interfaz de configuración en el sistema **Debian Sarge**. La interfaz será tras ello accesible en la dirección IP 192.168.100.24.

En el apéndice E.3, "*Instalación de la interfaz*", se encuentran las instrucciones para la instalación de la interfaz de configuración. Por otro lado, será necesario contemplar los aspectos presentados en los apéndices E.1.3, "*Ejecución de instrucciones con privilegios: sudo*", y E.1.4, "*Acceso a ficheros con privilegios restringidos*", para que la interfaz quede en estado totalmente operativo.

8. Durante algunas fases de las pruebas se dispuso de un segundo sistema **Debian Sarge** en el que se ejecutaba una sonda *fprobe-ng* adicional, que dirigía sus flujos hacia la dirección 192.168.100.24 y al puerto UDP 556. Con este segundo exportador se pudo comprobar el comportamiento de las aplicaciones en entornos con más de un exportador de información.

F.2. Pruebas de depuración realizadas sobre la interfaz

En esta sección se presentan una serie de pruebas realizadas sobre la interfaz de configuración de las distintas utilidades. Las pruebas indicadas se corresponden a usos intencionadamente erróneos de la interfaz para someterla a casos excepcionales, si bien durante el desarrollo de la mismas se hizo una utilización completa de las capacidades de la interfaz y, aunque no detallado en esta sección, el funcionamiento de la interfaz y de las utilidades manejadas fue el adecuado.

Pasamos pues a citar las pruebas concretas realizadas sobre cada uno de los módulos.

F.2.1. Depuración de la interfaz para *flow-capture*

Las siguientes pruebas, además de las de un uso normal del programa, se realizaron sobre el módulo de *flow-capture* obteniendo resultados satisfactorios:

1. Lectura y escritura del fichero de configuración

   a) Disponer de líneas de sintaxis no válida en el archivo de configuración de *flow-capture*. En tal caso se muestra un mensaje de error por pantalla y no se permite la ejecución normal de la interfaz.

   b) No tener definido ningún recolector en el archivo de configuración de *flow-capture*. En tal caso el recolector se muestra como «Parado» en el «Estado del recolector».

   c) Existencia de directivas no reconocidas en la definición de algún recolector en el archivo de configuración. Dichas directivas se conservarán en la configuración y no se modificarán a pesar de no mostrarse en el formulario.

2. Inserción de un nuevo recolector desde el formulario

   a) Introducir valores incorrectos en los campos para la inserción de un nuevo recolector. En tal caso se dará un error de validación en el formulario.

b) No especificar valores en todos los campos obligatorios del formulario. En tal caso se dará un error de validación.

c) Intentar establecer directorios con espacios en el campo «Directorio» en la inserción de un nuevo recolector, debido a que *flow-capture* no soporta directorios con espacios en su configuración. En tal caso se dará un error de validación.

d) Introducir un valor ya utilizado en los campos «Puerto» o «Directorio» en la inserción de un nuevo recolector. En tal caso se dará un error de validación.

3. Acciones provocadas desde módulos externos

   a) En caso de realizarse alguna modificación sobre la configuración de un recolector de *flow-capture* y estar *flow-capture* en ejecución, se procederá a la modificación de la configuración y a la aplicación de la nueva configuración a través del reinicio del servicio.

F.2.2. Depuración de la interfaz para *FlowScan*

Las siguientes pruebas, además de las de un uso normal del programa, se realizaron sobre el módulo de *FlowScan* obteniendo resultados satisfactorios:

1. Lectura y escritura del fichero de configuración

   a) Disponer de líneas de sintaxis no válida en el archivo de configuración de *FlowScan*. En tal caso se muestra un mensaje de error por pantalla y no se permite la ejecución normal de la interfaz.

   b) No estar analizando ningún recolector en el sistema. En tal caso se presenta un mensaje de aviso por pantalla y la interfaz no permite la ejecución del servicio. En caso de que además el servicio de *FlowScan* se encontrase en ejecución este se detendría.

2. Modificación de la configuración desde el formulario

   a) Introducir valores incorrectos en los campos para la inserción de nuevos elementos de la configuración del analizador. En tal caso se dará un error de validación en el formulario.

   b) No especificar valores en todos los campos obligatorios del formulario. En tal caso se dará un error de validación.

   c) Introducir un valor ya utilizado en los campos «Nombre del nuevo protocolo», «Nombre del nuevo servicio», «Nombre del nuevo ToS», «Nombre de la nueva red», «Nombre del nuevo exportador» o «Nombre del nuevo AS» en la inserción de nuevos elementos en la configuración. En tal caso se dará un error de validación.

3. Acciones provocadas desde módulos externos

   a) En caso de ser borrado un recolector que esté siendo analizado por *FlowScan* se procederá a la detención del procesado del mismo.