Apéndice A

Monitorización estadística de tráfico

Índice del capítulo

A.1. *NetFlow* versión 7

Como hemos comentado a lo largo del capítulo 4, "*Monitorización estadística de tráfico*", tanto la sonda que genera la información como el recolector que la recibe deben ser compatibles y utilizar la misma versión del *NetFlow*. En nuestro caso, la sonda y el recolector seleccionados son compatibles en usar las versiones 1, 5 y 7 del protocolo *NetFlow*.

Vamos a hacer en esta sección un acercamiento a la versión 7 del protocolo que es la más actual de las que pueden soportar ambas aplicaciones de sonda y recolector utilizados mostrando los campos de la cabecera y del registro en los Cuadros A.1 y A.2 respectivamente [5].

Bytes	***Contents***	***Description***
0-1	version	*NetFlow export format version number*
2-3	count	*Number of flows exported in this flow frame (protocol data unit, or PDU)*
4-7	SysUptime	*Current time in milliseconds since the export device booted*
8-11	unix_secs	*Current seconds since 0000 UTC 1970*
12-15	unix_nsecs	*Residual nanoseconds since 0000 UTC 1970*
16-19	flow_sequence	*Sequence counter of total flows seen*
20-23	reserved	*Unused (zero) bytes*

Cuadro A.1: Campos de la cabecera de *NetFlow* V7

Puede verse que la cabecera de *NetFlow* del Cuadro A.1 transporta información general, como `SysUptime` (tiempo que lleva operativo el sistema que genera el mensaje) o `unix_secs` (marca de tiempo formada por los segundos transcurridos desde el 1 de enero de 1970). El campo `count`, segundo de la cabecera, indica el número de registros que se entregan dentro de este mensaje. Esto se entenderá mejor con la siguiente explicación: una cabecera de *NetFlow* va acompañada de varios campos de datos, también llamados registros o en la literatura inglesa *flows*, como el que se muestra en el Cuadro A.2. Así, gracias al campo `count`, el receptor del mensaje sabe cuantos de estos *flows* debe buscar en el mensaje recibido.

Es gracias a los contenidos del registro de *NetFlow* del Cuadro A.2 cuando se puede entender lo referido en el punto 4.2.3, "*La sonda y el protocolo NetFlow*", donde comentábamos las peculiaridades de la sonda al manejar los contenidos de *NetFlow*. Campos como `nexthop` (siguiente encaminador o *router* de la ruta a seguir) o `src_as` (número del *sistema autónomo*[1] de origen) carecerían de sentido si la información es proveniente de un *sniffer* como es el caso de nuestra sonda. Además, merece resaltar que a pesar de estar definidos algunos de los campos no portan información al ser sus contenidos siempre «cero» y casualmente son muchos de los campos que nuestra sonda no podría utilizar adecuadamente.

[1]En la literatura consultada, un *sistema autónomo* o *AS* es una red o conjunto de redes que comparten una política común en cuanto a las reglas de encaminamiento. Habitualmente pertenece a una única entidad administrativa (como una universidad o división de una empresa) y a cada *AS* se le asigna de forma global un identificador numérico. Las redes dentro del *AS* comparten la información de encaminamiento con protocolos IGP y el *AS* la comparte con otros *AS* mediante BGP.

Bytes	***Contents***	***Description***
0-3	srcaddr	*Source IP address; in case of destination-only flows, set to zero.*
4-7	dstaddr	*Destination IP address.*
8-11	nexthop	*Next hop router; always set to zero.*
12-13	input	*SNMP index of input interface; always set to zero.*
14-15	output	*SNMP index of output interface.*
16-19	dPkts	*Packets in the flow.*
20-23	dOctets	*Total number of Layer 3 bytes in the packets of the flow.*
24-27	First	*SysUptime, in milliseconds, at start of flow.*
28-31	Last	*SysUptime, in milliseconds, at the time the last packet of the flow was received.*
32-33	srcport	*TCP/UDP source port number; set to zero if flow mask is destination-only or source-destination.*
34-35	dstport	*TCP/UDP destination port number; set to zero if flow mask is destination-only or source-destination.*
36	flags †	*Flags indicating, among other things, what flow fields are invalid.*
37	tcp_flags	*TCP flags; always set to zero.*
38	prot	*IP protocol type (for example, TCP = 6; UDP = 17); set to zero if flow mask is destination-only or source-destination.*
39	tos	*IP type of service; switch sets it to the ToS of the first packet of the flow.*
40-41	src_as	*Source autonomous system number, either origin or peer; always set to zero.*
42-43	dst_as	*Destination autonomous system number, either origin or peer; always set to zero.*
44	src_mask	*Source address prefix mask; always set to zero.*
45	dst_mask	*Destination address prefix mask; always set to zero.*
46-47	flags †	*Flags indicating, among other things, what flows are invalid.*
48-51	router_sc ⋆	*IP address of the router that is bypassed by the Catalyst 5000 series switch. This is the same address the router uses when it sends NetFlow export packets. This IP address is propagated to all switches bypassing the router through the FCP protocol.*

† Cambio sobre *NetFlow* version 5.

⋆ Adición sobre *NetFlow* version 5.

Cuadro A.2: Campos del registro de *NetFlow* V7

A.2. Instalación y configuración de la sonda

A.2.1. Instalación de *fprobe-ng*

Procedemos en este punto y en los siguientes al proceso de instalación y configuración de la sonda seleccionada, *fprobe-ng*.

Al estar disponible como *paquete Debian* la instalación es extremadamente sencilla:

```
#> apt-get install fprobe-ng
```

Con el siguiente comando se podrán consultar los contenidos del paquete:

```
#> dpkg -L fprobe-ng
```

A.2.2. Configuración de *fprobe-ng*

La sonda se puede configurar cómodamente atendiendo a su fichero de configuración en `/etc/default/fprobe-ng`. Así mismo, listamos el contenido por defecto del archivo de configuración para estudiar su contenido:

`/etc/default/fprobe-ng` (original)

```
#fprobe-ng default configuration file

INTERFACE="eth0"
FLOW_COLLECTOR="localhost:555"

#fprobe can't distinguish IP packet from other (e.g. ARP)
OTHER_ARGS="-fip"
```

El archivo de configuración es leído por *fprobe-ng* en su arranque, y son simplemente parámetros de la línea de comandos para la ejecución del programa. Podríamos ejecutar *fprobe-ng* igualmente llamando a su binario y dándole una idéntica lista de parámetros a los que podemos encontrar en el archivo de configuración.

También hay que comentar que ***fprobe-ng*** emplaza una *script* de arranque en `/etc/init.d` para que su arranque se produzca junto al arranque del sistema.

Para entender mejor el archivo de configuración vamos a presentar los parámetros principales de configuración de *fprobe-ng* como se indica en el Cuadro A.3. Para más información acerca de estos y otros parámetros puede consultarse el manual del programa [10].

Hacemos ahora las siguientes consideraciones referentes a la estructura de nuestra red que nos servirán de ejemplo para plasmar una configuración concreta en la utilidad:

- La sonda va a escuchar en modo promiscuo en la interfaz eth0 de una máquina de nuestra red.
- La sonda enviará la información a un recolector que escuchará en la máquina 192.168.100.24 de nuestra red, en el puerto 555.

Parámetro	**Descripción**
-i `interface`	Interfaz en la que *fprobe-ng* escuchará en modo promiscuo.
-n `version`	Versión del protocolo *NetFlow* a utilizar. Soporta las versiones 1,5 y 7. Por defecto utilizará la 5.
-f `expression`	Sentencia en formato *tcpdump* que se utilizará para filtrar la captura de datos.
`remote:port`	Indican la dirección IP y el puerto donde el recolector espera el flujo de *NetFlow*. *fprobe-ng* puede mandar la misma información a más de un recolector.

Cuadro A.3: Parámetros de *fprobe-ng*

- La sonda enviará los datos sobre *NetFlow* versión 7, compatible con el recolector.

Tras esta descripción, listamos finalmente el contenido de nuestro archivo de configuración:

`/etc/default/fprobe-ng` (modificado)

```
#fprobe-ng default configuration file

INTERFACE="eth0"
FLOW_COLLECTOR="192.168.100.24:555"

#fprobe can't distinguish IP packet from other (e.g. ARP)
OTHER_ARGS="-fip -n 7"
```

De esta forma, la sonda escuchará en modo promiscuo en el interfaz seleccionado y mandará hacia el recolector ubicado en el puerto 555 del sistema con dirección IP 192.168.100.24 la información generada a través de *NetFlow* versión 7.

A.3. Instalación y configuración del recolector

A.3.1. Instalación de *flow-tools*

Procedemos en este punto y en los siguientes al proceso de instalación y configuración del paquete de herramientas para el manejo de *NetFlow* ***flow-tools***.

Como también se provee en un *paquete Debian*, su instalación es simple y rápida:

```
#> apt-get install flow-tools
```

El contenido del paquete se podrá listar con la siguiente orden:

```
#> dpkg -L flow-tools
```

A.3.2. Configuración de *flow-capture*

Nos centraremos en este punto únicamente en el recolector *flow-capture* comprendido dentro del paquete ***flow-tools***. Su configuración se establece en el archivo `/etc/flow-tools/flow-capture.conf`. De dicho fichero, listamos su contenido por defecto:

`/etc/flow-tools/flow-capture.conf` (original)

```
# Configuration for flow-capture
#
# Robin Elfrink <robin@a1.nl>
#
# Every line is basically just the options to flow-capture, see
# flow-capture(1) for explanation.


# Example 1:
# Capture flows from router at 10.1.1.10, listening at port 3000.
# Store flows in /var/flow/myrouter.
-w /var/flow/myrouter 0/10.1.1.10/3000

# Example 2:
# Capture flows from router at 10.3.2.6, listening at port 3002.
# Store flows in /var/flow/mysecondrouter. Rotate files every
# 5 minutes.
-w /var/flow/mysecondrouter -n 275 0/10.3.2.6/3002

# Example 3:
# Same as above, but only listen at address 10.3.2.5, and store
# files under 'YYYY/YYYY-MM/YYYY-MM-DD' directories.
-w /var/flow/mysecondrouter -n 275 -N 3 10.3.2.5/10.3.2.6/3002
```

Como puede verse, el fichero está claramente comentado y facilita su comprensión, pero aun así comentamos algunos de sus parámetros de configuración principales en el Cuadro A.4. Para más información, véase su manual [15].

Tengamos en cuenta los siguientes puntos sobre la estructura de la red:

- La máquina que va a alojar al recolector es la misma que la que aloja a la sonda, es decir, se aloja en la dirección IP 192.168.100.24.
- La sonda usada y el recolector son compatibles en utilizar las versiones de *NetFlow* 1, 5 y 7, y se seleccionará esta última versión dado que fue la elegida en la configuración de la sonda.

Parámetro	**Descripción**
-w `workdir`	Especifica el directorio principal donde el recolector almacenará la información proveniente de la sonda.
-n `rotations`	Indica el número de ficheros que almacenará *flow-capture* durante un día, o lo que es lo mismo el intervalo temporal para guardar la información en el disco. El valor por defecto es 95, es decir, crea un archivo cada 15 minutos.
-e `expire_count`	Número de archivos máximo a almacenar por el recolector. En caso de sobrepasarse se procede a la eliminación de los más antiguos. Se comprobarán todos los subdirectorios del directorio principal del recolector.
-E `expire_size`	Tamaño máximo ocupado por los archivos capturados por el recolector. En caso de sobrepasarse se procede a la eliminación de los más antiguos. Se comprobarán todos los subdirectorios del directorio principal del recolector.
-v `pdu_version`	Especifica la versión de *NetFlow* a usar.
-N `nesting_level`	Indica el formato de anidamiento de los archivos: -3 YYYY/YYYY-MM/YYYY-MM-DD/flow-file -2 YYYY-MM/YYYY-MM-DD/flow-file -1 YYYY-MM-DD/flow-file 0 flow-file 1 YYYY/flow-file 2 YYYY/YYYY-MM/flow-file 3 YYYY/YYYY-MM/YYYY-MM-DD/flow-file Por defecto el valor es 3.
`localip/remoteip/port`	Establece la dirección local donde se escuchará, la dirección remota a la que se aceptarán los flujos y el puerto donde se atienden las llegadas. Un valor 0 en los dos primeros hará válida cualquier dirección.

Cuadro A.4: Parámetros de *flow-capture*

Con todo esto, mostramos finalmente nuestro fichero de configuración:

`/etc/flow-tools/flow-capture.conf` (modificado)

```
# Configuration for flow-capture
#
# Robin Elfrink <robin@a1.nl>
#
# Every line is basically just the options to flow-capture, see
# flow-capture(1) for explanation.

# Capturamos flujos provenientes de 192.168.100.24 escuchando en
    192.168.100.24:555
# Esperamos NetFlow Version 7
# Almacenamos en /var/flow/eth0
-V 7 -w /var/flow/eth0 192.168.100.24/192.168.100.24/555
```

Por tanto, nos quedaría funcionando según el esquema mostrado en la Figura A.1.

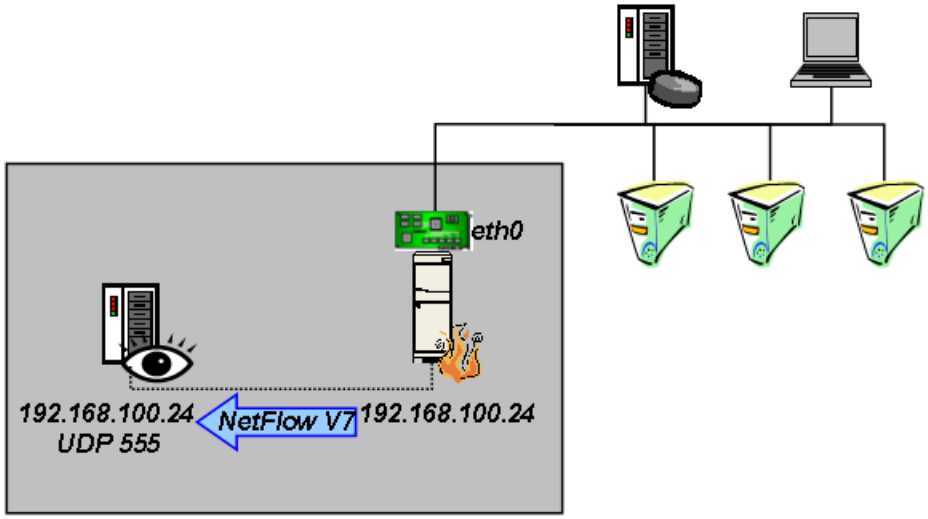

Figura A.1: Esquema de funcionamiento de la sonda y el recolector

Al igual que ocurría con ***fprobe-ng***, el archivo de configuración es leído en el arranque y equivale a introducir la misma línea de parámetros en la ejecución del binario. Así mismo se emplaza una *script* en `/etc/init.d` para su arranque con el sistema.

Por último, merece la pena resaltar que *flow-capture* solo aceptará la información de sondas que estén listadas en su archivo de configuración, lo que ofrece una seguridad nimia. Por ello recomendamos seguir las consideraciones realizadas en la sección 4.4, "*Consideraciones de seguridad para NetFlow*".