CAPÍTULO III

Implementación del protocolo Neflow y del software “Listry-AIGC”

3.1 Introducción

Netflow, como se describió en el capítulo uno, es un protocolo de monitoreo de red creado por Cisco que parcialmente se ha convertido en un estándar en el uso de esta tecnología. Actualmente otras marcas soportan el protocolo Netflow en sus dispositivos activos con algunas variantes, logrando un crecimiento considerable en el uso de este protocolo para el monitoreo de redes.

Nfsen, software libre elegido del proceso de investigación realizado en el capítulo dos, es un software encargado de mostrar todos los datos capturados por Nfdump en una interfaz web amigable para el usuario; además los creadores de Nfsen añadieron diversas utilidades al software, como son:

- Graficas
- Alertas
- Proceso de *background* mediante el uso de filtros.
- Observación específica sobre los datos capturados (profiles)
- Posibilidad de añadir programación exterior al software(creación de plugins)

En este capítulo se explica la implementación realizada del protocolo Netflow en la institución, así como el funcionamiento del software Nfdump y Nfsen.

3.2 Implementación del protocolo Netflow

Antes de habilitar el protocolo Netflow, fue necesario conocer el esquema de red que se tiene implementado en la institución. La figura 3.1 muestra el esquema general de la red implementado en la institución.

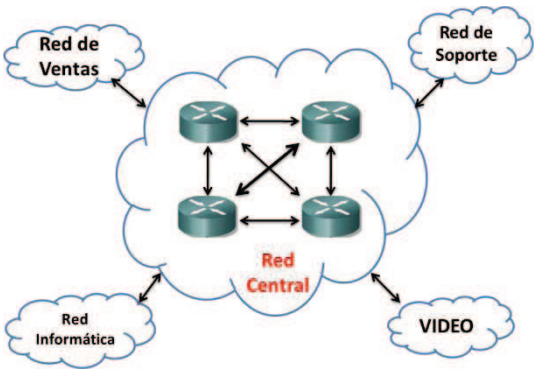


Figura 3.1 Esquema de red General

Como se observa en esta figura, se tienen cinco redes principales habilitadas: La red mostrada en el centro (Red Central) es la red principal de la institución. Esta red se encarga de las siguientes actividades:

- Interconexión con otras redes.
- Administración de redes de usuarios y servidores.
- Soporte a la operación, basado en las capas 2-4 del modelo OSI.

El esquema de red mostrado es aplicado en seis áreas de operación; se ha habilitado el protocolo Netflow en seis dispositivos activos asociados a un edificio específico. La figura 3.2

muestra el esquema de implementación del protocolo Netflow en la Red Central de la institución.

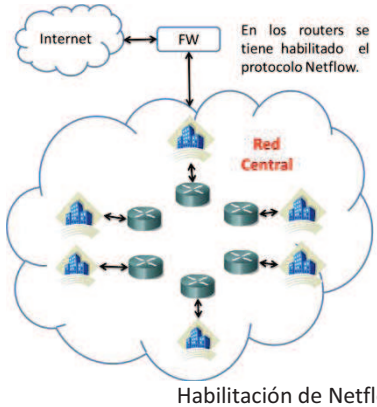


Figura 3.2 Habilitación de Netflow sobre RI

Como se observa en esta figura, cada router presente en la Red Central se encarga de proporcionar los servicios de red a un edificio en específico. En cada edificio se tienen creadas redes de usuarios, redes de servidores, redes de telefonía y otras redes de acuerdo al esquema de red mostrado en la figura ocho. Al habilitar el protocolo Netflow en estos routers se pretende tener un monitoreo constante (24*7) [Se pretende realizar un monitoreo 24 horas * 7 días a la semana, los 365 días del año], enfocado a observar las actividades realizadas en cada edificio, especialmente se observará el tráfico que circula en las redes de usuarios y servidores.

La figura 3.3 muestra las redes que tendrán una mayor observación mediante el monitoreo de red.

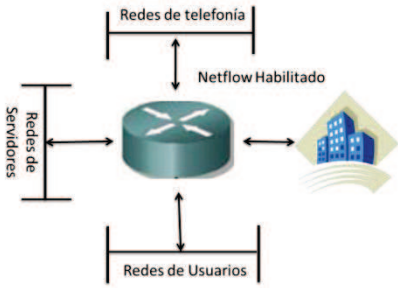


Figura 3.3 Redes a monitorear sobre los edificios.

Aunque se tiene implementado un esquema de seguridad robusto en la institución, las redes mencionadas son susceptibles a algún ataque realizado en ellas por usuarios internos o externos, esto ha motivado a que por medio del monitoreo de red, se realicé un algoritmo capaz de buscar anomalías presentes en estas redes, y que notifique inmediatamente al encontrar algún comportamiento inusual.

La estrategia del plugin creado en el software Nfsen, se describe en el capítulo IV, en la siguiente sección se describe como fue implementado el software “Listry-AIGC”.

3.3 Implementación del software "Listry-AIGC"

3.3.1 ¿Qué es el software Listry-AIGC?

El software "Listry-AIGC" es un conjunto de módulos instalados, enfocados en dos principales actividades.

- En el monitoreo de red.
- En la detección de malware que deja evidencia en la red y opera en capas inferiores del modelo OSI.

Los módulos y herramientas instalados en el software "Listry-AIGC", permiten al administrador de red mayor seguridad y comodidad al utilizar este software. Debido a que proporciona todas sus funcionalidades en forma gráfica. Los módulos y herramientas que incluye este software son los siguientes:

- Habilitación del protocolo Hypertext Transfer Protocol Secure (HTTPS).
- Instalación y configuración de MySQL.
- Instalación y configuración del software OpenWebmail.
- Instalación y configuración del software Navicat.
- Instalación y configuración del colector Nfdump.
- Instalación y configuración del software Nfsen.
- Configuración del plugin "escaneo" en el software Nfsen.

El software "Listry-AIGC" fue instalado en un S.O. Centos 5.5 virtualizado en VmWare server 2.0.

Los seis dispositivos activos configurados en el software Nfsen, envían los export packet generados por cada uno de ellos hacia el colector Nfdump cada cinco minutos, mediante el software Nfsen se logran visualizar los datos presentes en una interfaz web.

Además, para que el router funcione como un dispositivo exportador, es necesario activar el protocolo Netflow de la siguiente forma:

1. Entrar al router y acceder al modo privilegiado
   - router$ enable
2. Entrar al modo de configuración
   - router# configure terminal
3. Entrar a la interfaz en donde se habilitara Netflow (repetir del paso 3 al 5 si se pretende activarlo en todas las interfaces)
   - Router(config)# interface GigabitEthernet x/x
   - Donde:
     - x/x = Numero de la interfaz del router
4. Se habilita la recolección de flujos
   - Router(config-if)# ip route-cache flow
5. Regresar a modo de configuración
   - Router(config-if)# exit
6. Redirigir los paquetes UDP hacia el colector
   - Router(config)# ip flow-export destination yyy.yyy.yyy.yyy zzzzz
   - Donde:

- yyy.yyy.yyy.yyy = Ip del colector
- zzzzz = Puerto UDP

7. Configurar la interfaz de donde se enviaran los datos (repetir el paso siete si se enviaran datos de todas las interfaces)
   - Router(config)# ip flow-export source GigabitEthernet x/x
8. Elegir la versión del protocolo Neflow utilizada
   - Router(config)# ip flow-export version 9
   - NOTA: Si la v9 no es compatible con el router, utilizar la versión v5.
9. Opcional: Configurar timeout
   - Router(config)# ip flow-cache timeout active 1
   - Router(config)# ip flow-cache timeout inactive 15
10. Salir del modo de configuración
    - Router(config)# ctrl + Z
11. Guardar los cambios
    - Router# write mem

La configuración puede variar dependiendo del dispositivo activo donde se habilitará Netflow, sin embargo, se muestra la configuración general del protocolo Netflow en un equipo Cisco.

La figura 3.4 muestra el esquema general de envío de los export packets hacia el dispositivo colector.

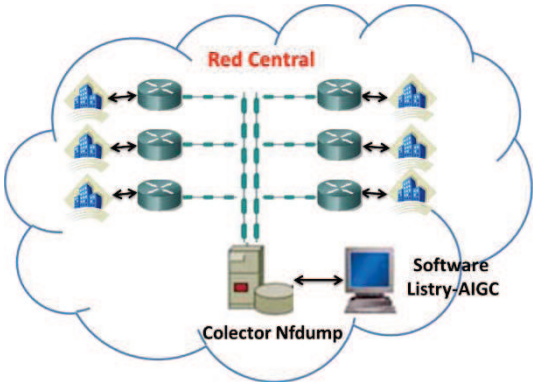


Figura 3.4. Envío de export packets hacia el colector.

Para poder utilizar al software “Listry-AIGC”, como una alternativa enfocada a sustituir al software Netflow comercial, e implementarse en la institución. Se sometió dicho software a las siguientes etapas:

1. Investigación: En esta etapa se investigó acerca del funcionamiento del software, Nfsen, los requisitos necesarios para su instalación y su funcionamiento (1 mes).
2. Instalación: En esta etapa se instaló el software Nfsen mediante el proceso qua ya se ha descrito (1 semana).
3. Pruebas: En esta etapa al software Nfsen se le asignó una dirección IP perteneciente a un laboratorio de pruebas dentro de Red Central, además se asoció un dispositivo activo con el objetivo de monitorear las redes del edificio asociado a este dispositivo las 24 horas del día. Esto se realizó con el objetivo observar el comportamiento del Software Nfsen; la respuesta ofrecida y para verificar algún error en su funcionamiento antes de pasarlo a la etapa de producción (6 meses)

4. Implementación/Producción. Una vez superada exitosamente la fase de pruebas se configuraron los cinco routers faltantes para que enviaran los Export Packets generados hacia el colector Nfdump, como se observa en la figura 3.5. Además se asignó al software Nfsen una IP perteneciente a una red de servidores, completando con esto la fase de implementación/Producción.

En este capítulo se explica minuciosamente el funcionamiento del software Nfdump y Nfsen. La descripción de los demás módulos instalados en el software "Listry-AIGC", se encuentra en el glosario C "Guía de usuario del software Listry-AIGC".

El software Nfsen realiza monitoreo de las actividades presentes en las redes de usuarios y servidores las 24 horas del día. Durante la fase de pruebas, el software Nfsen mostro un óptimo funcionamiento debido a que recibía los Export Packet generados por un router cada cinco minutos (un paquete recibido contenía en promedio 300 flujos), además de explotar las diversas funcionalidades ofrecidas por Nfsen, en beneficio de la institución, las cuales son:

- Creación de Profiles: Se crearon profiles enfocados en el monitoreo de redes de usuarios y redes de servidores, monitoreo de servicios y monitoreo de conexiones realizadas hacia servidores;
- Alertas: Se crearon alertas enfocadas en la detección de picos presentes en la red de la institución y;
- Plugin: Se creó un plugin enfocado en la detección de malware mediante patrones típicos de comportamiento.

3.3.2 Nfdump Definición

Nfdump es un software regido bajo licenciamiento BSD, que se encarga de recolectar e interpretar datos en formato Netflow provenientes de dispositivos exportadores. Actualmente el software Nfdump se encuentra en la versión 1.5.8 y soporta las versiones 5, 7 y 9 del protocolo Netflow.

El software Nfdump tiene un conjunto de herramientas para capturar y procesar datos en formato Netflow en línea de comandos, las cuales son:

- nfcapd: Demonio que captura los datos en formato Netflow.
- nfdump: Aplicación creada para procesar el conjunto de datos en formato Netflow capturados (ficheros generados por nfcapd).
- nfprofile: Filtra los datos en formato Netflow guardados en función de los perfiles definidos (profiles).
- nfreplay: Lee los datos en formato Netflow guardados en ficheros por nfcapd y los reenvía a otro equipo.
- nfclean.pl: Script para borrar datos antiguos.

Aunque hay multitud de herramientas creadas para leer, procesar y representar datos en formato Netflow tanto en línea de comandos como en formato gráfico, pocas de ellas tienen la flexibilidad y potencia ofrecida por el software Nfdump a la hora de procesar los datos. Está herramienta puede ser muy útil en:

- La detección de ataques hacia la red.

- Generación de reportes.
- Realizar análisis forenses.
- Obtener diversas estadísticas del uso de: BW, puertos, redes, servicios, etc.

La figura 3.5 muestra el funcionamiendo del software Nfdump [http://nfdump.sourceforge.net/]:

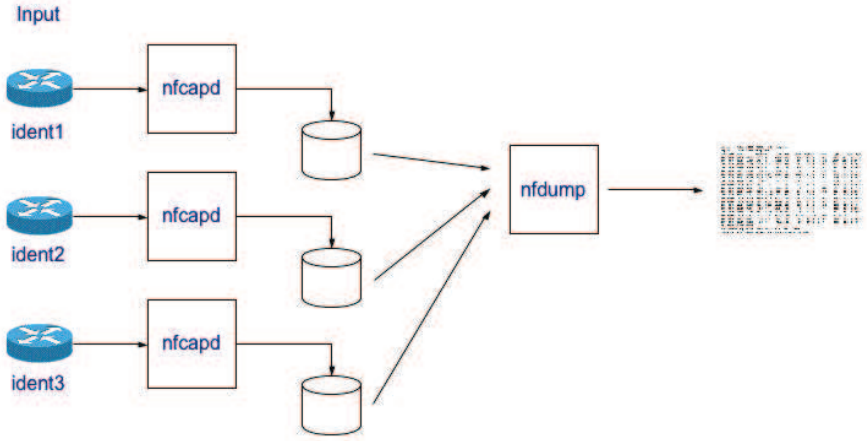


Figura 3.5 Funcionamiento nfdump

El comportamiento del software Nfdump se rige de la siguiente forma:

- El software Nfdump permite asociar uno o varios dispositivos exportadores que tienen habilitado el protocolo Netflow. Nfdump asocia a cada exportador un demonio nfcapd que se encarga de escuchar sobre un puerto UDP específico.
- El demonio nfcapd escucha y captura todos los Export Packets provenientes del dispositivo exportador asociados a él.
- Los Export Packets son enviados cada cinco minutos por el dispositivo exportador hacia el demonio Nfcapd que se ha asociado (se puede configurar el tiempo de envió de Export Packets). El colector Nfdump se encarga de guardar los Export Packets recibidos en archivos nfcapd (o en bases de datos, depende de la configuración realizada en la instalación del software Nfdump) que únicamente pueden ser interpretados por la herramienta nfdump.
- La herramienta nfdump se encarga de interpretar y mostrar toda la información guardada por nfcpad en texto claro. Además sobre esta herramienta se pueden aplicar filtros muy específicos con el objetivo de realizar un análisis detallado sobre los datos presentes.

3.3.2.1 Nfcapd funcionamiento

Nfcpad es el demonio encargado de recolectar los datos provenientes de los exportadores y almacenarlos cada cinco minutos en un archivo con el siguiente formato:

nfcapd.AAAAMMDDHHMINMIN (ej.: nfcapd.201008291420)

Estos archivos solo pueden ser interpretados por la herramienta nfdump y contienen información acerca de los flujos capturados por el exportador que los ha generado.

En la figura 3.6 se muestran algunos archivos capturados; estos archivos se generan automáticamente cada cinco minutos y contienen los flujos almacenados por el equipo exportador.

```
[root@localhost ll]# ls
nfcapd.201003110000  nfcapd.201003110155  nfcapd.201003110350  nfcapd.201003110545  nfcapd.201003110740
nfcapd.201003110005  nfcapd.201003110200  nfcapd.201003110355  nfcapd.201003110550  nfcapd.201003110745
nfcapd.201003110010  nfcapd.201003110205  nfcapd.201003110400  nfcapd.201003110555  nfcapd.201003110750
nfcapd.201003110015  nfcapd.201003110210  nfcapd.201003110405  nfcapd.201003110600  nfcapd.201003110755
nfcapd.201003110020  nfcapd.201003110215  nfcapd.201003110410  nfcapd.201003110605  nfcapd.201003110800
nfcapd.201003110025  nfcapd.201003110220  nfcapd.201003110415  nfcapd.201003110610  nfcapd.201003110805
```

Figura 3.6 Archivos nfcpad.

Al momento de añadir los equipos exportadores en el archivo de configuración del software Nfsen, Este software se encargará de configurar automáticamente el demonio nfcapd asociado al dispositivo exportador

Si es necesario configurar manualmente el demonio nfcapd, se realiza de la siguiente forma:

#nfcapd -w -D -l /flow_base_dir/exportador -p 23456

Dónde:

- W: Tiempo de rotación de los archivos (5 minutos por defecto)
- D: Background (Demonio)
- l: Directorio de salida
- Flow_base_dir: Directorio que contiene los archivos capturados
- Exportador: Nombre del equipo a observar

Para mayor información sobre las banderas utilizadas por nfcapd, teclear sobre shell:

#nfcapd –h

3.3.2.2 El intérprete nfdump

La herramienta nfdump sirve como un intérprete de los datos capturados por Nfcapd. Sus funciones principales son las siguientes.

- Ver el contenido de uno o varios archivos nfcpad.
- Realizar un análisis sobre los archivos seleccionados por medio de filtros basados en expresiones regulares.
- Visualizar el resultado de forma clara para el usuario o guardarlo en un archivo nfcapd.

El funcionamiento de la herramienta nfdump se muestra en la figura 3.7.

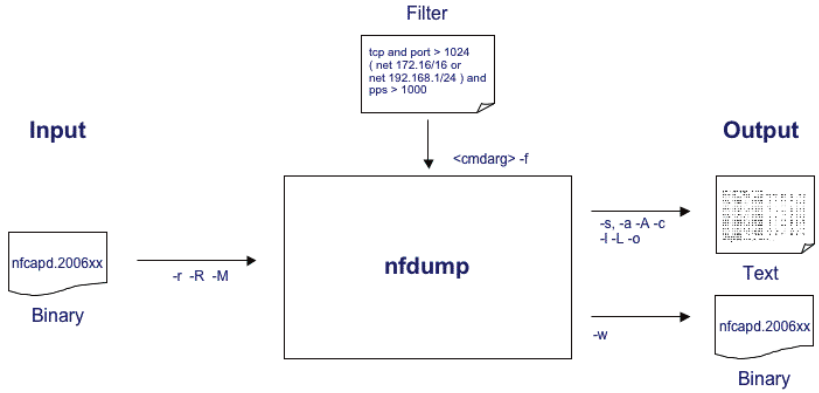


Figura 3.7 Procesamiento de datos Nfdump.

El procesamiento de datos mediante la herramienta nfdump se basa en:

- La lectura de archivos capturados por nfcapd mediante –r, -R o –M dependiendo del tipo de lectura:
  - -r: Solo lee un archivo;
  - -R: Lee un conjunto de archivos que se encuentran en el mismo directorio (/dir:file1:file2);
  - -M: Lee archivos desde múltiples directorios (/dir/dir1:dir2:dir3)
- El realizar un análisis detallado mediante la aplicación de filtros, acotando la información.
  - -z 'Filtro a aplicar';
  - Consultar el anexo C para mayor información de la sintaxis de los filtros.
- El modo de salida que puede ser:
  - Mostrar los datos en pantalla (-S –a –A –c –l –L –o);
  - Guardar los datos en un nuevo archivo (-w).

Las opciones descritas son las banderas básicas utilizadas por la herramienta nfdump. Cabe mencionar lo potente que es el software Nfdump en la realización de análisis background, en la detección de picos presentes sobre las redes, saber qué Ip's consumen mayor ancho de banda y en análisis enfocados sobre seguridad informática. Para mayor información sobre otras banderas teclear en Shell

```
# nfdump -h
```

3.3.2.3 Ejemplos de la herramienta nfdump.

En esta sección se proporcionan tres ejemplos sobre el uso de la herramienta nfdump.

1. Leer los datos de un archivo generado con la fecha 12-Marzo-2010 15:20

Solución: `# nfdump –r nfcapd.201003121520`

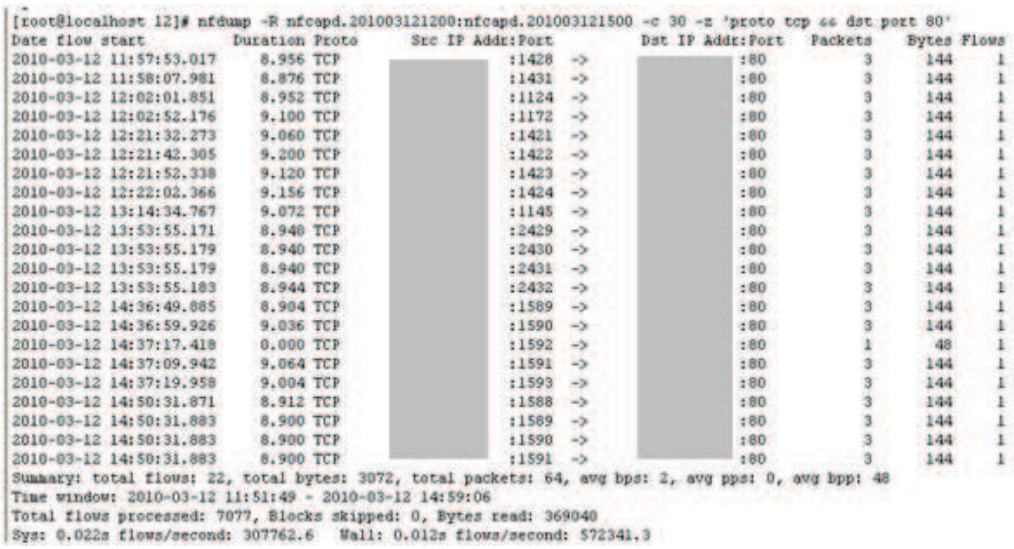
Nota: Se tendrá que estar situado en el directorio donde se encuentra el archivo o hacer referencia a él.

```
[root@localhost 12]# nfdump -r nfcapd.201003121520
Date flow start          Duration Proto      Src IP Addr:Port          Dst IP Addr:Port   Packets    Bytes Flows
2010-03-12 15:14:07.256     3.000 UDP      [redacted]          ->      [redacted]               2      656     1
2010-03-12 15:14:07.268     3.000 UDP                          ->                               2      656     1
2010-03-12 15:14:15.460     0.000 UDP                          ->                               1       87     1
2010-03-12 15:14:24.060     0.000 UDP                          ->                               1       68     1
2010-03-12 15:14:24.424     0.000 UDP                          ->                               1       68     1
2010-03-12 15:14:28.064     0.000 UDP                          ->                               1       68     1
2010-03-12 15:14:28.428     0.000 UDP                          ->                               1       68     1
2010-03-12 15:14:30.268     0.000 UDP                          ->                               1      229     1
2010-03-12 15:10:01.560   299.244 UDP                          ->                            3078   332424     1
2010-03-12 15:14:36.988     0.000 UDP                          ->                               1       84     1
2010-03-12 15:14:41.476     0.000 UDP                          ->                               1       87     1
2010-03-12 15:14:35.992     9.000 TCP                          ->                               3      152     1
2010-03-12 15:14:50.376     0.000 UDP                          ->                               1      229     1
2010-03-12 15:14:42.084     8.948 TCP                          ->                               3      144     1
2010-03-12 15:14:55.940     0.000 ICMP                         ->                               1       92     1
2010-03-12 15:14:45.316    14.504 UDP                          ->                               2      400     1
2010-03-12 15:15:02.105     0.000 UDP                          ->                               1       68     1
2010-03-12 15:15:03.201     0.000 UDP                          ->                               1       68     1
2010-03-12 15:15:06.109     0.000 UDP                          ->                               1       68     1
2010-03-12 15:15:07.209     0.000 UDP                          ->                               1       68     1
2010-03-12 15:15:07.413     0.000 UDP                          ->                               1      576     1
2010-03-12 15:15:07.493     0.000 UDP                          ->                               1       87     1
```

Figura 3.8 Resultado del ejemplo 1

Leer los datos de flujos que se obtuvieron el 12-Marzo-2010 entre las 12:00 y 15:00, mostrando solo los 30 primeros flujos que presentaron actividad en el protocolo TCP y enviaron datos a través de http.

Solución: #nfdump -R nfcapd.201003121200:nfcapd.201003121500 -c 30 -z 'proto tcp && dst port 80'



```
[root@localhost 12]# nfdump -R nfcapd.201003121200:nfcapd.201003121500 -c 30 -z 'proto tcp && dst port 80'
Date flow start          Duration Proto      Src IP Addr:Port           Dst IP Addr:Port   Packets    Bytes Flows
2010-03-12 11:57:53.017     8.956 TCP                  :1428  ->                  :80         3      144     1
2010-03-12 11:58:07.981     8.876 TCP                  :1431  ->                  :80         3      144     1
2010-03-12 12:02:01.851     8.952 TCP                  :1124  ->                  :80         3      144     1
2010-03-12 12:02:52.176     9.100 TCP                  :1172  ->                  :80         3      144     1
2010-03-12 12:21:32.273     9.060 TCP                  :1421  ->                  :80         3      144     1
2010-03-12 12:21:42.305     9.200 TCP                  :1422  ->                  :80         3      144     1
2010-03-12 12:21:52.338     9.120 TCP                  :1423  ->                  :80         3      144     1
2010-03-12 12:22:02.366     9.156 TCP                  :1424  ->                  :80         3      144     1
2010-03-12 13:14:34.767     9.072 TCP                  :1145  ->                  :80         3      144     1
2010-03-12 13:53:55.171     8.948 TCP                  :2429  ->                  :80         3      144     1
2010-03-12 13:53:55.179     8.940 TCP                  :2430  ->                  :80         3      144     1
2010-03-12 13:53:55.179     8.940 TCP                  :2431  ->                  :80         3      144     1
2010-03-12 13:53:55.183     8.944 TCP                  :2432  ->                  :80         3      144     1
2010-03-12 14:36:49.885     8.904 TCP                  :1589  ->                  :80         3      144     1
2010-03-12 14:36:59.926     9.036 TCP                  :1590  ->                  :80         3      144     1
2010-03-12 14:37:17.418     0.000 TCP                  :1592  ->                  :80         1       48     1
2010-03-12 14:37:09.942     9.064 TCP                  :1591  ->                  :80         3      144     1
2010-03-12 14:37:19.958     9.004 TCP                  :1593  ->                  :80         3      144     1
2010-03-12 14:50:31.871     8.912 TCP                  :1588  ->                  :80         3      144     1
2010-03-12 14:50:31.883     8.900 TCP                  :1589  ->                  :80         3      144     1
2010-03-12 14:50:31.883     8.900 TCP                  :1590  ->                  :80         3      144     1
2010-03-12 14:50:31.883     8.900 TCP                  :1591  ->                  :80         3      144     1
Summary: total flows: 22, total bytes: 3072, total packets: 64, avg bps: 2, avg pps: 0, avg bpp: 48
Time window: 2010-03-12 11:51:49 - 2010-03-12 14:59:06
Total flows processed: 7077, Blocks skipped: 0, Bytes read: 369040
Sys: 0.022s flows/second: 307762.6   Wall: 0.012s flows/second: 572341.3
```

Figura 3.9 Resultado del ejemplo 2

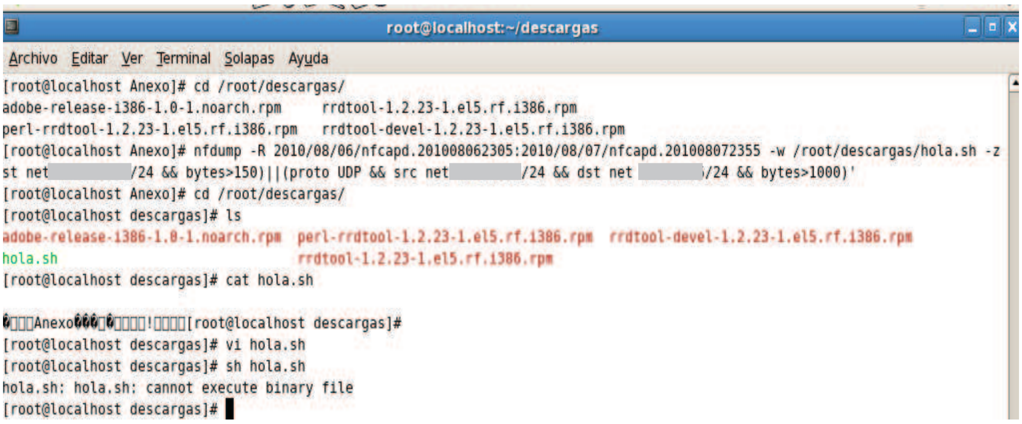
2. Leer los datos en el siguiente periodo de tiempo 06-Agosto-2010 23:05 a 07-Agosto-2010 23:55, limitándolo a 200 flujos con las siguientes condiciones:
    - Únicamente bandera habilitada de inicio de sesión sobre la subred x.x.x/24 con un tamaño mayor a 150 bytes.
    - O todo lo que pasa a través de UDP de la subred z.z.z/24 hacia y.y.y/24 con un tamaño mayor a 1000 bytes
    - El resultado guardarlo en /root/descargas con el nombre de 'hola.sh'

Solución:

#nfdump -R 2010/08/06/nfcapd.201008062305:2010/08/07/nfcapd.201008072355 -w /root/descargas/hola.sh -c 50 –z '(flags S && not flags APF && dst net x.x.x/24 && bytes >150) || (proto UDP && src net z.z.z/24 && dst net y.y.y/24 && bytes >1000)'

El resultado del comando aplicado será la generación del archivo "*hola.sh*"; este archivo creado solo podrá ser observado mediante nfdump: Si se quiere observar su contenido mediante algún editor de textos (o los comandos, vi, cat, more, etc.), la información contenida en este archivo será mostrada en forma ilegible hacia el usuario. De igual manera si se desea ejecutar el archivo "*hola.sh*" (por medio de sh ó ./), el shell notificara que no es un archivo ejecutable.

En la figura 3.10 se observa que no es posible acceder al contenido del archivo hola.sh por los medios tradicionales:



Al ejecutar Vi, la salida fue la siguiente:

```
^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@
@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^
^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@
@^@^@^@^@^@^@ÿÿÿ^?^@^@^@^@c^C^@^@^@^@^@^@^A^@^@^@^T^@^@^@^B^@^@^@!^B^@^P^@^@^@^H^@^D^@^F^@^@^@^@^@^Q^@^@
```

Figura 3.10 Esconder datos con ayuda de nfdump

Como se observa la ejecución del comando nfdump crea un archivo disfrazado e ilegible con otros lectores de archivos. Destaqué esta funcionalidad de nfdump debido a que me parece muy útil como una técnica de *esteganografía*.

Al ejecutar el archivo "hola.sh" mediante nfdump, se podrá observar toda la información que tiene nuestro archivo disfrazado. El resultado se observa en la figura dieciséis.

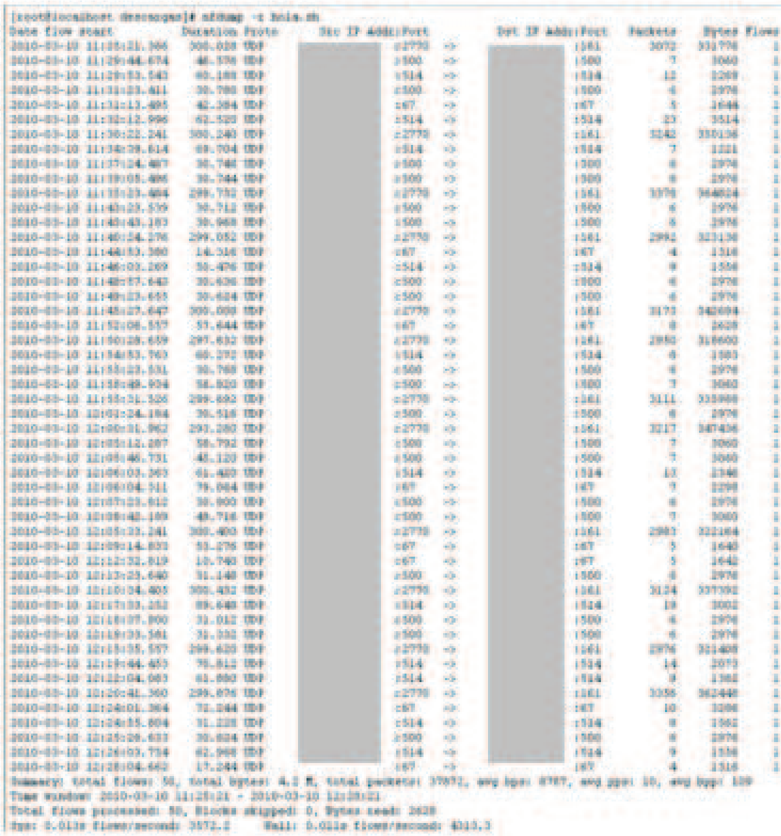


Figura 3.11 Salida del archivo hola.sh

3.3.3 Nfsen *Definición y funcionamiento*

El software Nfsen tiene el objetivo de proporcionar una interfaz gráfica al software Nfdump, además, Nfsen cuenta con las siguientes características:

- Muestra los datos almacenados por el demonio Nfcapd en graficas desglosadas de acuerdo a flujos, paquetes y el tráfico generado en los protocolos TCP, UDP, ICMP.
- Proporciona un ambiente web de fácil utilización.
- Permite observar y procesar los datos Netflow en lapsos de tiempo específicos.
- Actualización de las gráficas cada cinco minutos.
- Permite aplicar filtros para observar información acotada (utiliza la misma sintaxis soportada por Nfdump).
- Permite la creación de vistas específicas de los datos en formato Netflow (profiles) que pueden ser históricos o continuos.
- Permite la creación de alertas basadas en varias condiciones o en la ejecución de alertas mediante algún plugin.
- Permite añadir plugins para procesar datos de Netflow de acuerdo a las necesidades requeridas

En el anexo C “Guía de usuario Nfsen” se explica a detalle la configuración y utilización del software Nfsen.

3.3.3.1 Funcionamiento de Nfsen

El software Nfsen se encarga de graficar todos los datos obtenidos por el colector Nfdump, además de permitirnos opciones adicionales, como se ha descrito anteriormente. En la figura 3.12 se muestra el funcionamiento general del software Nfsen.

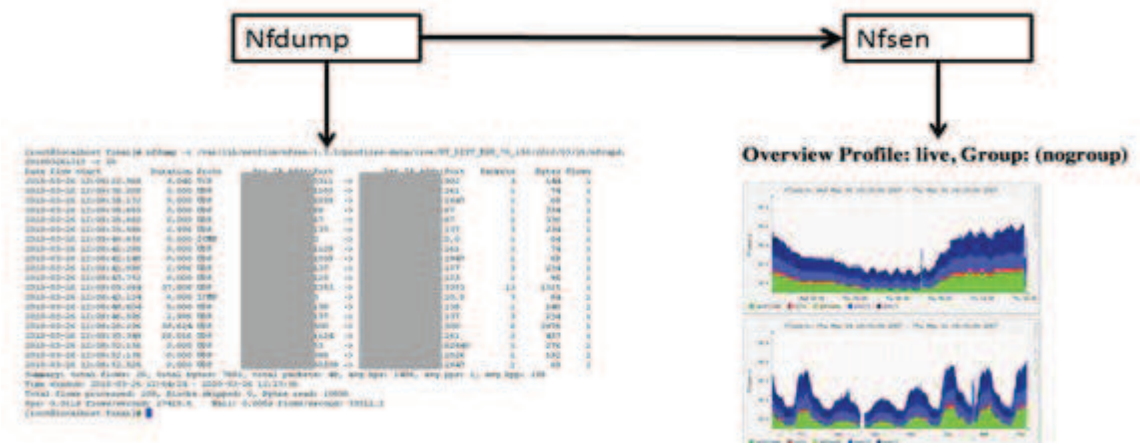


Figura 3.12 Funcionamiento nfsen

Cada archivo nfcapd obtenido por el colector Nfdump será mostrado y clasificado en las gráficas creadas por Nfsen automáticamente. Al desplazarse sobre una gráfica se muestra la fecha que hace referencia al punto específico observado; al dar clic en el Export Packet donde se encuentre posicionado el mouse se observará una tabla que contiene características generales de la cantidad de flujos, paquetes y tráfico presente en ese lapso de tiempo específico, además de permitir la aplicación de filtros para la realización de análisis y observar los datos del mismo modo que los presenta la herramienta nfdump.

Nfsen provee una gran flexibilidad en la visualización de los datos debido a que podemos observarlos de manera gráfica o en modo texto (mediante la herramienta nfdump). Además en sus tablas creadas se muestra el promedio de flow/s, paquetes/s y trafico/s de los protocolos TCP, UDP, ICMP y otros, asi como el tráfico consumido por estos mismos.

La figura 3.13 muestra un ejemplo de los Export Packets obtenidos en comparación con el tiempo y el tráfico consumido, tanto para una sola captura (archivo de 5 minutos) como para un lapso de tiempo en específico.

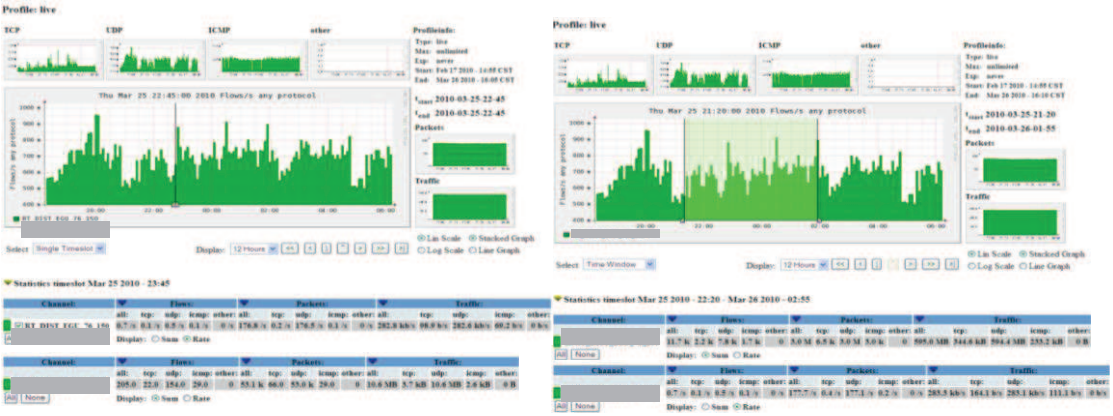


Figura 3.13 Presentación de datos

Desglosando esta imagen se observa un monitoreo constante del dispositivo exportador: las imágenes mostradas fueron obtenidas en el mismo lapso de tiempo; la diferencia entre ambas radica en observar en la imagen de la izquierda las estadísticas generadas por un solo Export Packet (archivo nfcapd.201003252345), mientras que en la imagen de la derecha se muestran las estadísticas generadas por un conjunto de Export Packets (archivos nfcapd 201003252220 al nfcapd 201003260255).

El poder observar un conjunto de Export Packets es de gran utilidad si se desea realizar un análisis sobre un lapso de tiempo específico, donde se haya presentado un aumento en el BW inusual al tráfico promedio obtenido. Además las tablas mostradas contienen la suma de todos los Export Packets observados en el lapso de tiempo específico y estas tablas son desglosadas de la manera descrita anteriormente.

El análisis sobre los datos en formato Netflow se realiza por medio de la aplicación de filtros (bajo la sintaxis descrita en el anexo C) y las diversas opciones incorporadas en el software Nfsen. Esto proporciona una gran potencia al software Nfsen en la investigación de eventos ocurridos, además de la posible detección de malware presente sobre la red y la pasible detección de malware de día cero.

3.3.3.2 Profiles

Como se explica en el anexo C Nfsen permite crear vistas personalizadas (profiles) con el objetivo de realizar observaciones específicas sobre los datos. Nfsen permite crear dos tipos de profiles:

- *Históricos:* Observación de datos en el pasado; se establece un punto inicial y un punto final para la observación de los datos.

- *Continuos:* Se empiezan a observar los datos en el pasado pero se continúan actualizando conforme se obtienen nuevos datos (el profile se actualizará cada cinco minutos).

La figura 3.14 se muestra un profile creado para monitorear redes de interés, tomando en cuenta la red origen y la red destino. El profile creado es de tipo continuo.

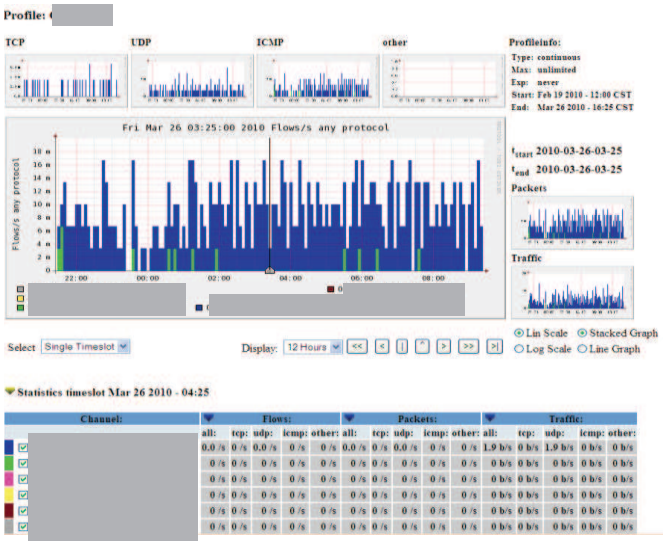


Figura 3.14 Ejemplo profile.

Desglosando esta figura, se observa que el profile creado separa las redes contenidas en el dispositivo exportador en los rangos establecidos en los filtros. A cada canal creado en el profile se le asignaron diversos filtros, logrando como resultado la gráfica mostrada que contiene las redes separadas. Cada color mostrado en la gráfica es resultado de una dirección IP perteneciente a una red de usuarios que adquiere un servicio proporcionado por una dirección IP perteneciente red de servidores.

Los profiles son de gran uso en el software Nfsen, debido a que permiten separar la información de acuerdo a las necesidades requeridas, por ejemplo:

- Observar el tráfico generado únicamente por redes de usuarios.
- Observar la utilización de puertos conocidos.
- Observar las conexiones realizadas hacia redes de servidores.
- Clasificar las conexiones realzadas en los puertos, conocidos, reservados y privados.
- Clasificar las conexiones realizadas de redes de usuarios hacia puertos bien conocidos.
- Entre otros.

3.3.3.3 Alertas

Otra característica a destacar del software Nfsen es la generación de alertas. Esta utilidad es de gran importancia debido a que permite mediante la aplicación de filtros, o algún plugin ejecutado en la alerta el detectar patrones anormales presentes en la red. Como puede ser:

- Detección de malware sobre la red.
- Aumento en el tráfico sin razón aparente.
- Host que consumen un mayor BW al asignado.
- Envío de información hacia redes no permitidas

- Utilización elevada de puertos conocidos, privados o reservados
- Entre otros.

Para mayor información acerca de la creación de una alerta y los estados de ejecución, consultar el anexo C.

En la figura 3.16 se muestra una alerta llamada conexión. Esta alerta monitorea las conexiones realizadas por cualquier cliente perteneciente a una red de usuarios y para su ejecución será necesario que se cumplan con las siguientes condiciones:

- Los flujos con los valores más altos (top 1) que excedan de 2 bits.
- Los paquetes con los valores más altos (top 1) que excedan de 10 Kb
- El tráfico con los valores más altos (top 1) que exceda de 10 Kb

Para que se ejecute y envíe un correo electrónico notificando, será necesario que todas sus condiciones sean verdaderas después de cinco ciclos (25 minutos).

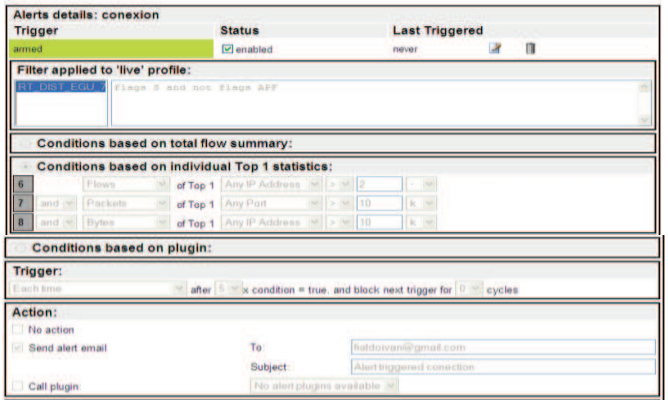


Figura 3.15 Creación de alerta.

La figura 3.15 tiene el objetivo de mostrar la configuración requerida para la creación de la alerta. En esta figura se observa un recuadro de color verde con la leyenda “armed”: Su significado es que la alerta se encuentra en ejecución, buscando que las condiciones programadas sobre ella se cumplan.

La figura 3.16 muestra la alerta creada en ejecución. En esta figura se observa una gráfica que contiene información acerca del promedio obtenido de los Export Packets (en el último ciclo; el promedio de 10 y 30 minutos anteriores; el promedio de 1, 4, 12 y 24 hora(s) anteriores, etc.). Además se observan dos tablas indicando lo siguiente:

- En la primera tabla se indica el valor (numérico) del promedio calculado por la alerta, tanto para los flujos, paquetes y bytes obtenidos en los lapsos de tiempo mencionados anteriormente.
- En la segunda tabla se observa el valor (booleano) devuelto por las condiciones creadas. El software Nfsen realiza una comparación AND sobre los resultados obtenidos de las condiciones; solamente la alerta se activará o pasará a otro estado de ejecución cuando todas las condiciones sean verdaderas.

Las alertas se actualizan cada cinco minutos, al igual que todas las funcionalidades del software Nfsen. En el ejemplo mostrado será necesario que la alerta se active cinco veces de forma consecutiva para cambiar al estado “fired” y que se ejecute.

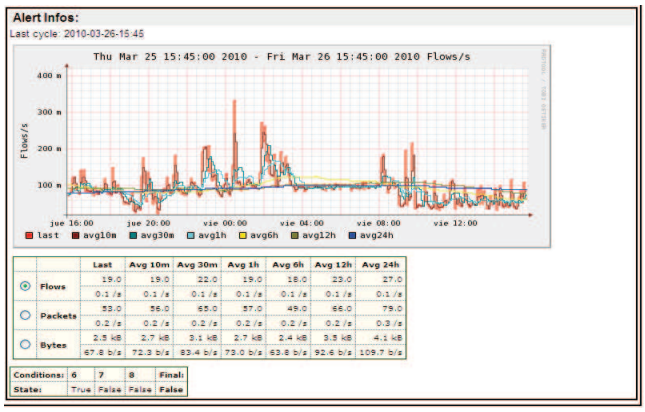


Figura 3.16 Ejecución de la alerta.

Las alertas pueden ser programadas para la ejecución de algún plugin con el objetivo de analizar por qué se presentó ese comportamiento anormal, brindando una mayor potencia al software Nfsen.

3.3.3.4 Plugins.

Los plugins son una potente herramienta utilizada por el software Nfsen, que permiten añadir programación exterior de acuerdo a las necesidades requeridas. Por medio de plugins creados en Nfsen se logra hacer a este software tan potente como se desee; además de enfocarlo hacia análisis de seguridad, poner precio al tráfico consumido, generar gráficas muy detalladas, entre otras cosas.

Nfsen soporta dos tipos de plugins:

- Backend: Módulos creados en perl con el objetivo de realizar acciones requeridas por el usuario y que no sean soportadas por Nfsen. Los plugin creados pueden ser enfocados de las siguientes maneras:
  - Condiciones de ejecución sobre alertas: Programación creada con el objetivo de cumplir condiciones creadas por el usuario y que no son soportadas directamente por Nfsen. Ejemplo: Monitorear si el ancho de banda se encuentra fuera del límite calculado por una línea base (baseline).
  - Acción específica al ejecutarse alguna alerta: Cuando las condiciones de ejecución en alguna alerta se cumplen, Nfsen lanzara el plugin creado bajo esta condición. Generalmente los plugin creados bajo esta acción buscaran, por medio del algoritmo creado, la causa de ejecución del plugin.
  - Actualización constante sobre nfsen: El plugin bajo esta condición se ejecutará en cada actualización de Nfsen (5 minutos por defecto). Dependiendo de la programación creada en el plugin, este podrá analizar cada archivo nfcapd obtenido en la última actualización de Nfsen, o analizar un conjunto de archivos nfcapd. Esta opción es muy utilizada cuando se programan algoritmos con el objetivo de buscar actividades anormales en la

red, o algoritmos que generan gráficas específicas y deben de ser actualizadas constantemente.

- Combinación de los puntos mencionados. Un pluglin creado bajo esta condición puede ser una combinación de las tres opciones mencionadas. Generalmente es usado sobre alertas: Se deberán de cumplir las condiciones programadas sobre el plugin para la ejecución de la alerta, así como al ejecutarse la alerta se lanzará el mismo plugin para verificar porque se ha presentado este comportamiento.

- Frontend: Programación creada sobre PHP con el objetivo de mostrar los resultados obtenidos en la ejecución del plugin backend asociado a él. Por ejemplo: al crear un plugin backend llamado "filtro.pm", el plugin generará como resultado un archivo de texto que contendrá el resultado de filtros programados sobre él; el plugin "filtro.php" tendrá como principal objetivo mostrar el contenido del archivo creado, sobre la interfaz web en Nfsen.

En el anexo C se muestra la programación necesaria para enfocar al plugin sobre alguna acción descrita en Backend, o el crear un plugin Frontend.

Como se ha descrito los plugins son una excelente herramienta utilizada en Nfsen. Por medio de la creación de plugins el software Nfsen se puede volver muy robusto e inclusive igualar o superar el funcionamiento de alguna alternativa propietaria.

En este trabajo de tesis se ha creado un plugin enfocado en la detección de malware presente en la red. El plugin fue creado para que se ejecute en cada actualización del software Nfsen analizando el último archivo nfcapd obtenido en búsqueda de algún comportamiento anormal sobre la red típico de un malware. Además se creó un módulo frontend con el objetivo de mostrar los resultados obtenidos del análisis realizado por el módulo backend. En el capítulo IV se explicara a detalle el funcionamiento del plugin creado.

La figura 3.17 muestra un plugin simple creado con el objetivo de mostrar el contenido del último archivo nfcapd obtenido.

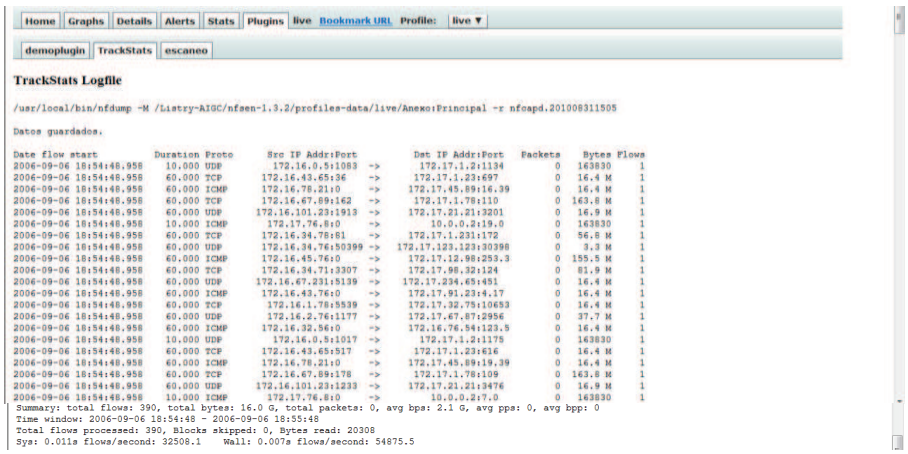


Figura 3.17 Ejecución de un plugin sobre nfsen.

Como se observa, los plugins pueden ser enfocados hacia cualquier funcionalidad requerida. Cada plugin creado en el software Nfsen permite añadir nuevas aplicaciones a este software,

enfocándolo hacia otras actividades diferentes al monitoreo de red, como puede ser la detección de malware presente la red, generación de gráficas de acuerdo con las necesidades, calcular costos por BW consumido, entre otros.

El plugin llamado "Trackstat", mostrado en la figura 3.17, se compone de los siguientes módulos:

- "Trackstat.pm": Módulo encargado de la obtención del último archivo nfcapd generado y guardarlo sobre un archivo de texto.
- "Trackstat.php": Módulo encargado de mostrar en la interfaz web el contenido del archivo creado por "Trackstat.pm".

El plugin "Trackstat" se ejecuta en cada actualización del software Nfsen, obteniendo el último archivo generado por nfcapd e interpretándolo.

En conclusión con todo lo mostrado acerca del funcionamiento del software Nfsen, se ha logrado cumplir con el objetivo de encontrar una alternativa Open Source capaz de sustituir en buena medida a software que requiere licenciamiento de uso. En este caso al software comercial utilizado en la institución Netflow. Además de ser la mejor alternativa software libre encontrada por los siguientes motivos.

- Software Libre.
- Soporta completamente el colector nfdump.
- Posibilidad de observar el código fuente y realizar mejoras sobre él.
- Foros web.
- Interfaz web amigable hacia el usuario.
- Las gráficas muestran los datos en lapsos de tiempo (12 horas, 1 día, 4 días, 1 semana, 1 mes; se pueden añadir más graficas con diferentes lapsos de tiempo).
- Las gráficas separan los datos de acuerdo a flujos, paquetes y tráfico contenido sobre los protocolos TCP, UDP, ICMP y otros.
- Actualización de datos constante.
- Posibilidad de realizar análisis sobre los datos presentes mediante filtros.
- Sobre cada Export Packet obtenido, se pueden observar las redes que consumen mayor ancho de banda (por medio de top n).
- Cataloga la información en base al ancho de banda consumido o el promedio con respecto al tiempo.
- Posibilidad de crear profiles.
- Creación de alertas y notificación.
- Creación de módulos compatibles con nfsen (plugins).
- Creación de alertas basadas en algoritmos (plugin enfocado hacia alertas).