



Gestión de Red

NfSen



These materials are licensed under the Creative Commons *Attribution-Noncommercial 3.0 Unported* license (<http://creativecommons.org/licenses/by-nc/3.0/>)

Qué es NfSen

- Una interfaz web para NfDump
- NfDump – Herramientas para recopilar y procesar flujos en la línea de comandos
- NfSen le permite:
 - Navegar con facilidad por los datos de NetFlow.
 - Procesar los datos dentro de una ventana de tiempo.
 - Crear archivos históricos y perfiles continuos.
 - Configurar alertas basadas en ciertas condiciones.
 - Escribir sus plugins propios para procesar los flujos cada cierto tiempo.

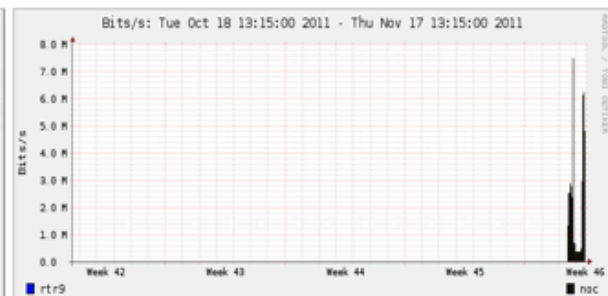
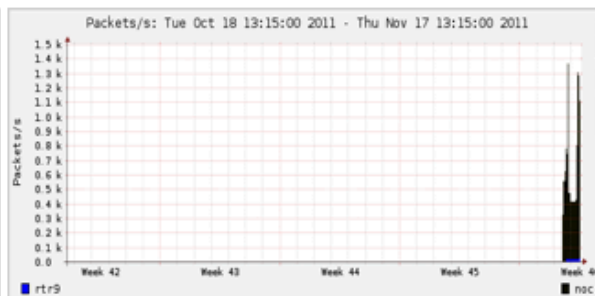
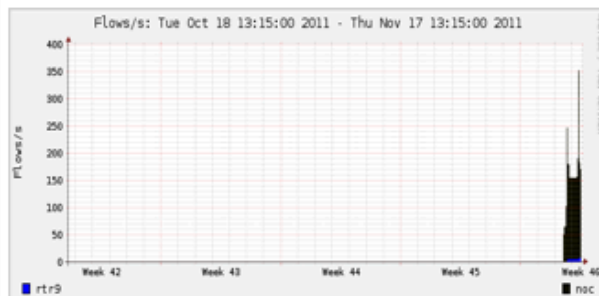
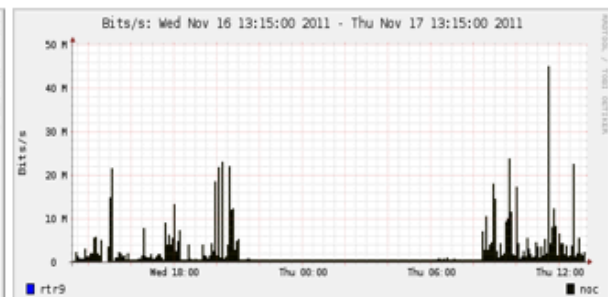
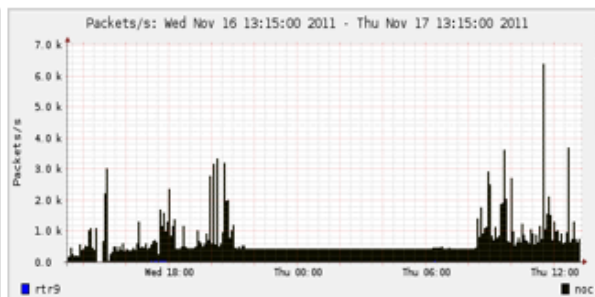
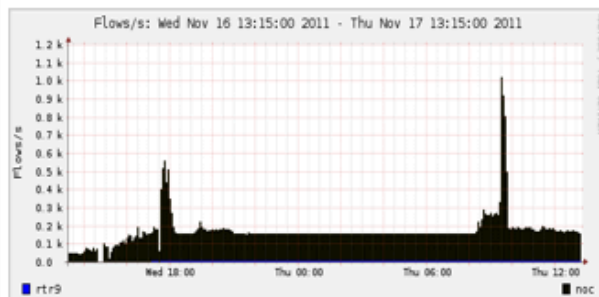
Estructura de NfSen

- Configuration file - nfsen.conf
- Archivos NfDump – Archivos que contiene flujos, almacenados en el directorio 'profiles-data'
 - Otras herramientas son capaces de leer archivos NfDump, pero no los guarde por mucho tiempo o se le llenará el disco duro.
- Los gráficos se guardan en el directorio 'profiles-stat'

Página de inicio de NfSen

[Home](#)[Graphs](#)[Details](#)[Alerts](#)[Stats](#)[Plugins](#)[live](#)[Bookmark URL](#)[Profile:](#)[live ▼](#)

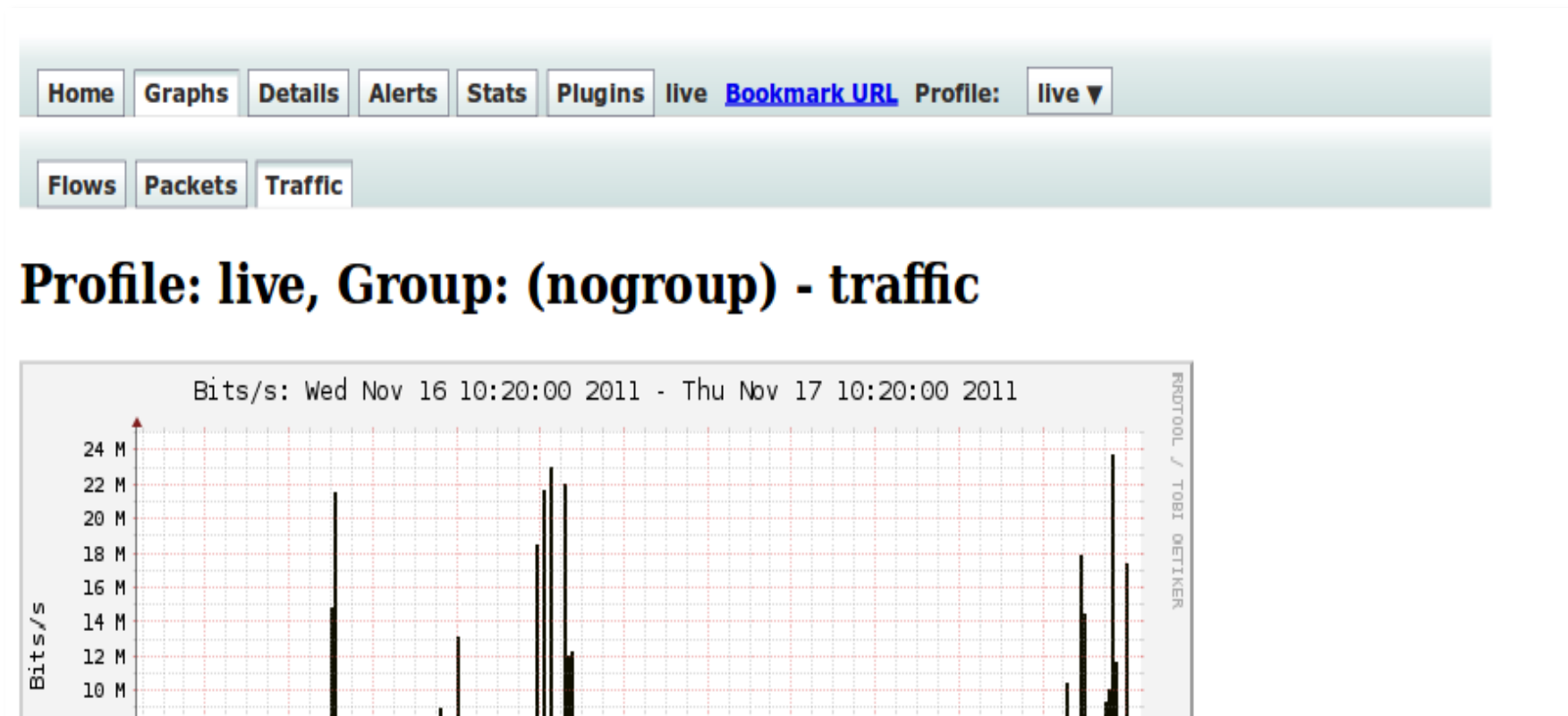
Overview Profile: live, Group: (nogroup)



Pestaña Graphs

Gráficos de flujos, paquetes y tráfico basados en interfaces con Netflow activo

El gráfico de tráfico debe corresponder con lo que muestra Cacti (SNMP) para la misma interfaz



Página de detalles

- La página más interesante
- Puede ver la información de flujos presentes o guardados
- Puede ver detalles como:
 - Números de AS (sólo útil si tiene una tabla de rutas BGP en su enrutador)
 - Nodos y puertos de fuente y destino
 - Flujos unidireccionales or bi-direccionales
 - Flujos de interfaces específicas
 - Protocolos y TOS



Gráficos del tráfico Netflow organizado por protocolo

Periodo del tiempo por los flujos en observación.

Gráfico del tráfico Netflow por todo los protocolos.

Routers bajo monitoreo

Opciones extendidas de procesamiento de Netflow.

Alertas y Estadísticas

Página de Alertas

- Puede crear alertas basadas en umbrales, ej. Incremento o decremento del tráfico
- Pueden enviarse e-mails

Página de Estadísticas

- Puede crear gráficos basados en ciertos criterios
 - ASNs,
 - Nodo, IPs destino, puertos
 - Interfaces de entrada/salida
 - Entre otros

Plugins

Existen varios plugins:

- **Porttracker** muestra los 10 puertos más activos (top ten)
- **Surfmap** Muestra el tráfico en un mapa geográfico

Más plugins aquí

<http://sourceforge.net/apps/trac/nfsen-plugins/>

PortTracker

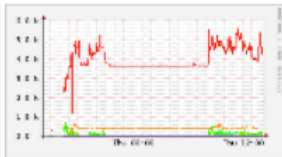
PortTracker

Port Tracker

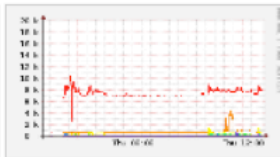
TCP Packets



TCP Flows



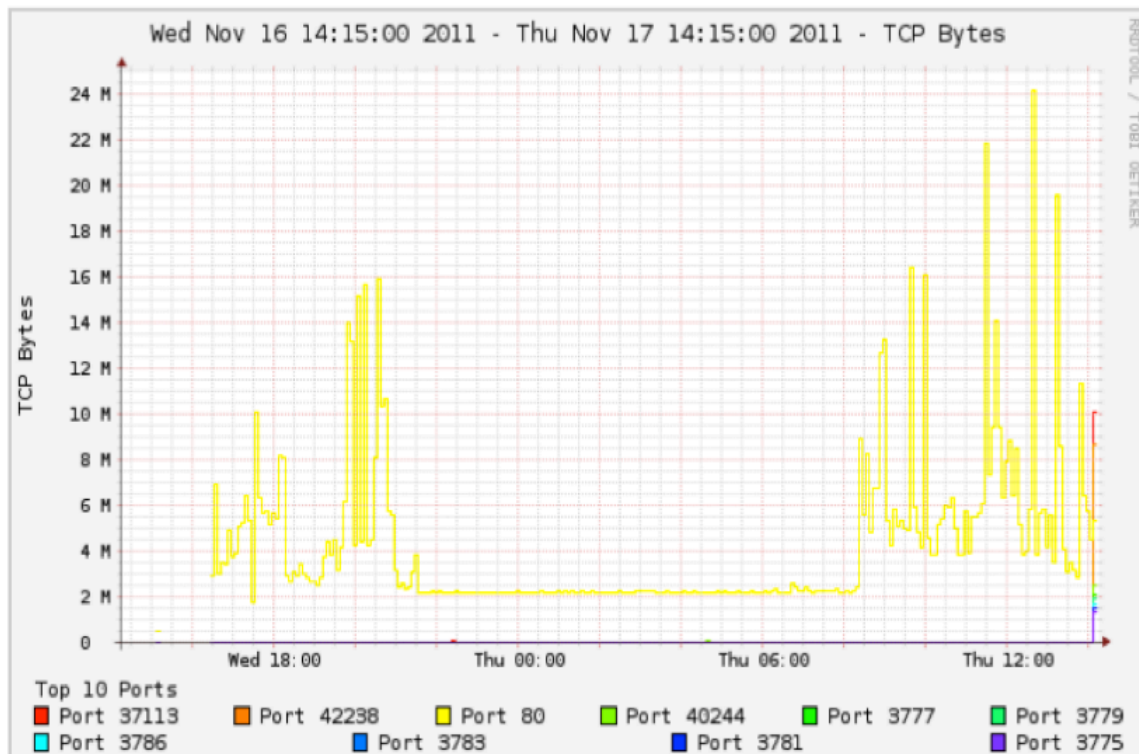
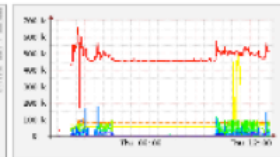
UDP Flows



UDP Packets



UDP Bytes



Show Top 10 Ports

☒ now ☐ 24 hours

Track Ports:

Add

Delete

Skip Ports:

Add

Delete

SurfMap



Cuando usar NfSen

- Puede usarse para:
 - Investigación forense: qué tráfico y qué nodos estaban activos en un momento específico
 - Ver tráfico de entrada/salida entre AS, tráfico entre IPs o puertos fuente/destino
 - Identificar los protocolos más usados
- Complementa a Cacti para ver información más detallada acerca del tipo de tráfico
- Con esta información puede tomar decisiones, ej:
 - Tiene una alta tasa de tráfico SNMP: puede que algunas máquinas estén enviando SPAM
 - 80% del tráfico es hacia ASN X: Puede que tenga sentido hacer peering con esa red para ahorrar costos de tránsito.



Tráfico unidireccional vs. bidireccional tal como es visto por NfSen

Unidireccional vs. Bidireccional

- Unidireccional muestra flujos desde A hasta B, y luego desde B hasta A
- Bidireccional muestra flujos entre A y B, combinados
- Puede combinarse con cualesquiera otros filtros (src port, src host más otros)
- La lista de filtros de puede encontrar en:
 - <http://nfsen.sourceforge.net/#mozTocId652064>

Bidireccional

All None Display: ☐ Sum ☒ Rate

Netflow Processing

Source: noc
rtr9

Filter: host 71.200.202.189

and <none>

Options:

☐ List Flows ☒ Stat TopN

Top: 10

Stat: Flow Records order by bytes

☒ bi-directional

Aggregate

proto

srcPort srcIP

dstPort dstIP

Limit: Packets > 0 -

Output: auto / IPv6 long

Clear Form process

```
** nfdump -M /var/nfsen/profiles-data/live/noc -T -R 2011/11/17/nfcapd.201111170930:2011/11/17/nfcapd.201111170950 -n 10 -s record/bytes
nfdump filter:
host 71.200.202.189
Command line switch -s overwrites -a
Aggregated flows 1
Top 10 flows ordered by bytes:
Date flow start      Duration Proto      Src IP Addr:Port      Dst IP Addr:Port      Out Pkt   In Pkt   Out Byte   In Byte   Flows
2011-11-17 09:34:12.206 1037.378 UDP        10.10.0.51:51413 <-> 71.200.202.189:57912    20077    19436    21.3 M    16.7 M    27455

Summary: total flows: 27455, total bytes: 38.0 M, total packets: 39513, avg bps: 292911, avg pps: 38, avg bpp: 961
Time window: 2011-11-17 08:22:09 - 2011-11-17 09:54:59
Total flows processed: 1061200, Blocks skipped: 0, Bytes read: 55106720
```


Unidirectional

All NONE Display: ☐ Sum ☒ Rate

Netflow Processing

Source: noc
rtr9
All Sources

Filter: host 71.200.202.189
and <none>

Options:
☐ List Flows ☒ Stat TopN
Top: 10
Stat: Flow Records order by bytes
☐ bi-directional
Aggregate ☒ proto ☒ srcPort ☒ dstPort
Limit: ☐ Packets > 0
Output: auto / IPv6 long
Clear Form process

```
** nfdump -M /var/nfsen/profiles-data/live/noc -T -R 2011/11/17/nfcapd.201111170930:2011/11/17/nfcapd.201111170950 -n 10 -s record/byte
nfdump filter:
host 71.200.202.189
Aggregated flows 2
Top 10 flows ordered by bytes:
Date flow start      Duration  Proto   Src IP Addr Src Pt   Dst IP Addr Dst Pt   Packets  Bytes    bps    Bpp  Flows
2011-11-17 09:34:12.380 1037.204  UDP     71.200.202.189 57912    10.10.0.51 51413    20077   21.3 M   164298 1060 14035
2011-11-17 09:34:12.206 1037.102  UDP     10.10.0.51 51413    71.200.202.189 57912    19436   16.7 M   128674 858 13420

Summary: total flows: 27455, total bytes: 38.0 M, total packets: 39513, avg bps: 292911, avg pps: 38, avg bpp: 961
Time window: 2011-11-17 08:22:09 - 2011-11-17 09:54:59
Total flows processed: 1001200, Flows skipped: 0, Bytes read: 55100700
```

Referencias

NfSen

<http://nfsen.sourceforge.net>

NfDump

<http://nfdump.sourceforge.net/>



Ejercicios