Gestión de Redes

NfSen

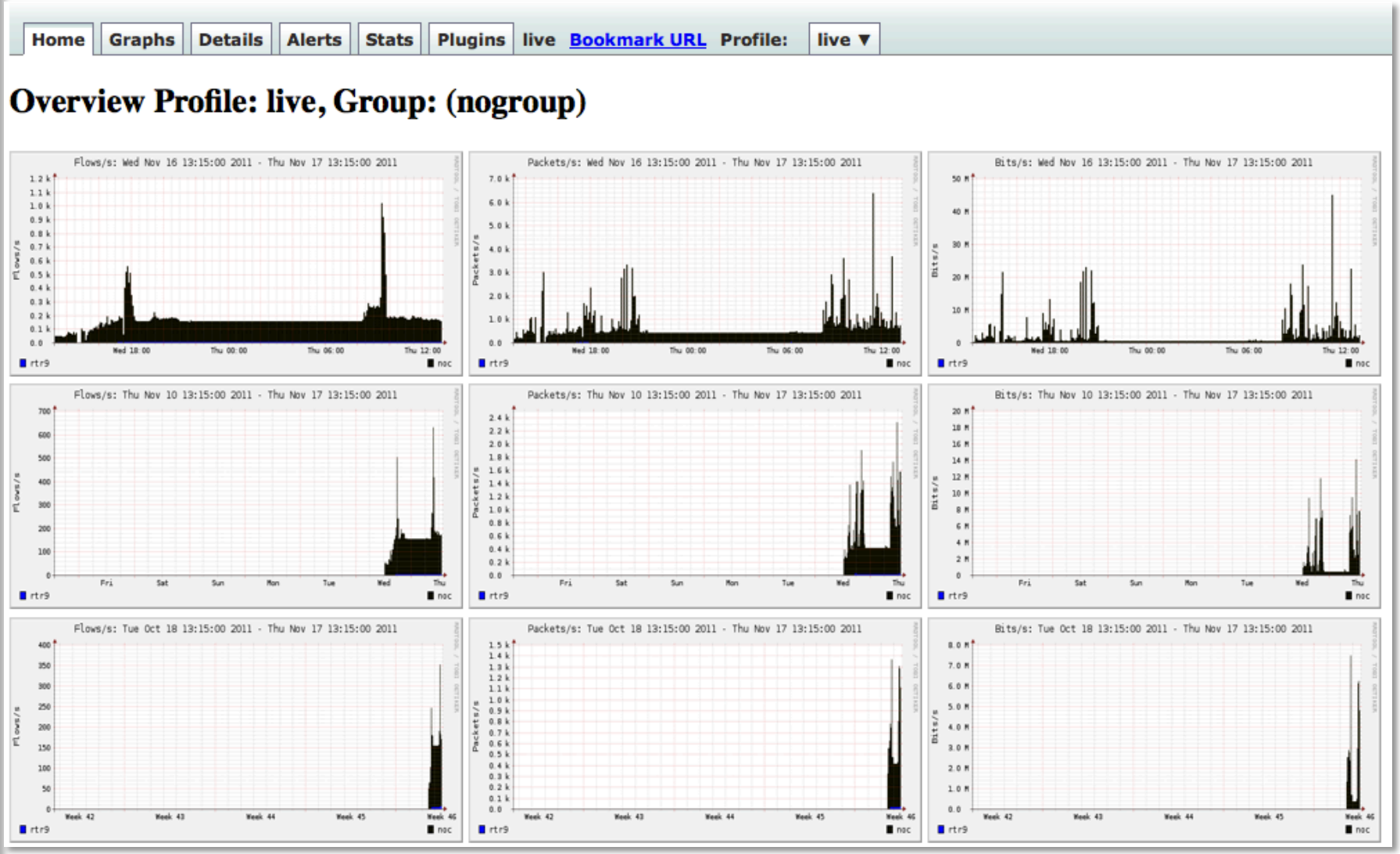
Qué es NfSen

- 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 propios plugins para procesar los flujos cada cierto tiempo.

Estructura de NfSen

- Archivo de configuracion - **nfsen.conf**
- Archivos NfDump – Archivos que contienen flujos almacenados en el directorio '**profiles-data**'
  - Otras herramientas son capaces de leer archivos NfDump, pero no los almacenan por mucho tiempo ya que se podria llenar el disco duro.
- Los gráficos se guardan en el directorio '**profiles-stat**'

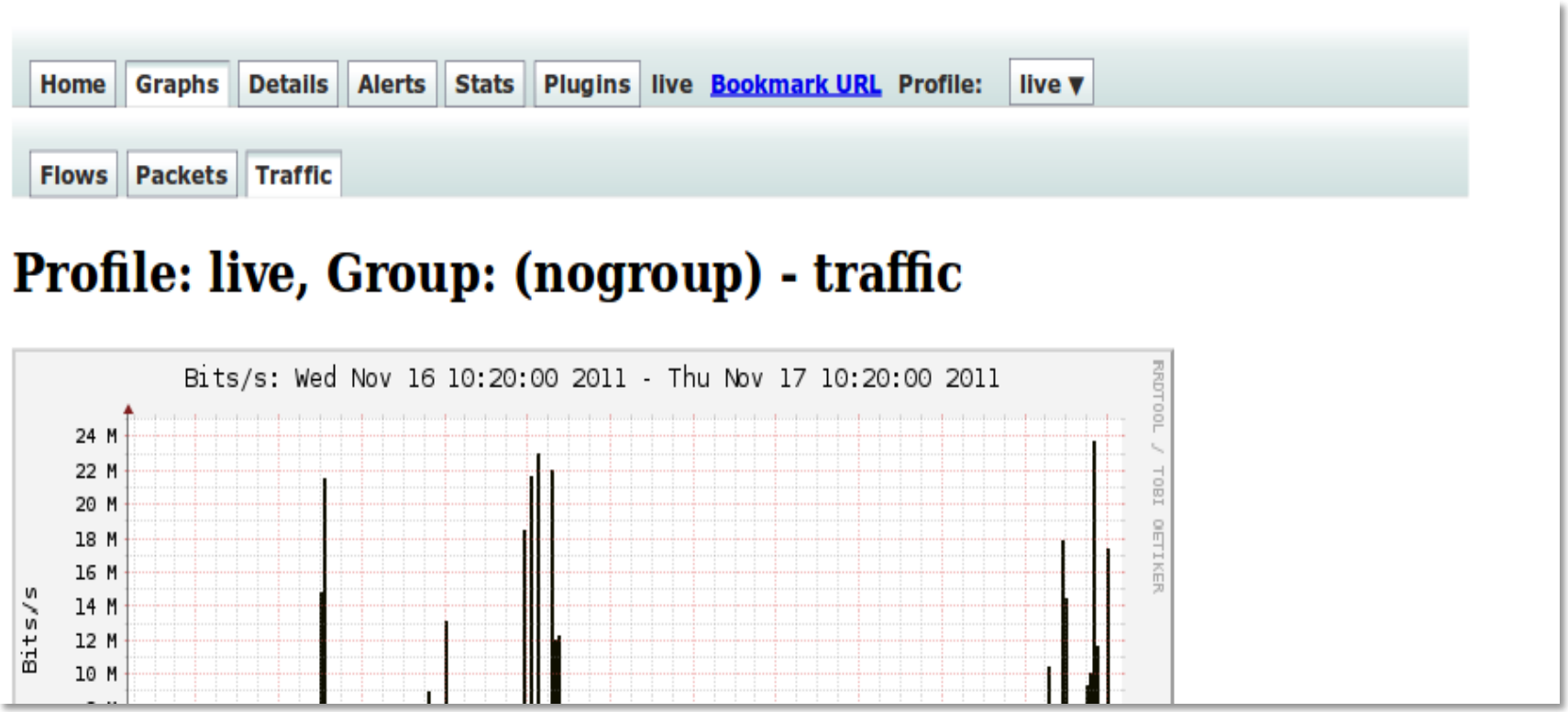
Página de inicio de NfSen



Pestaña de Graficos

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 Sistemas Autonomos AS (sólo útil si tiene una tabla de rutas BGP en su enrutador)
  - Nodos y puertos de origen y destino
  - Flujos unidireccionales or bi-direccionales
  - Flujos de interfaces específicas
  - Protocolos y TOS

Gráficos del trafico Netflow organizado por protocolo

Periodo del tiempo por los flujos en observación.

Gráfico del trafico 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

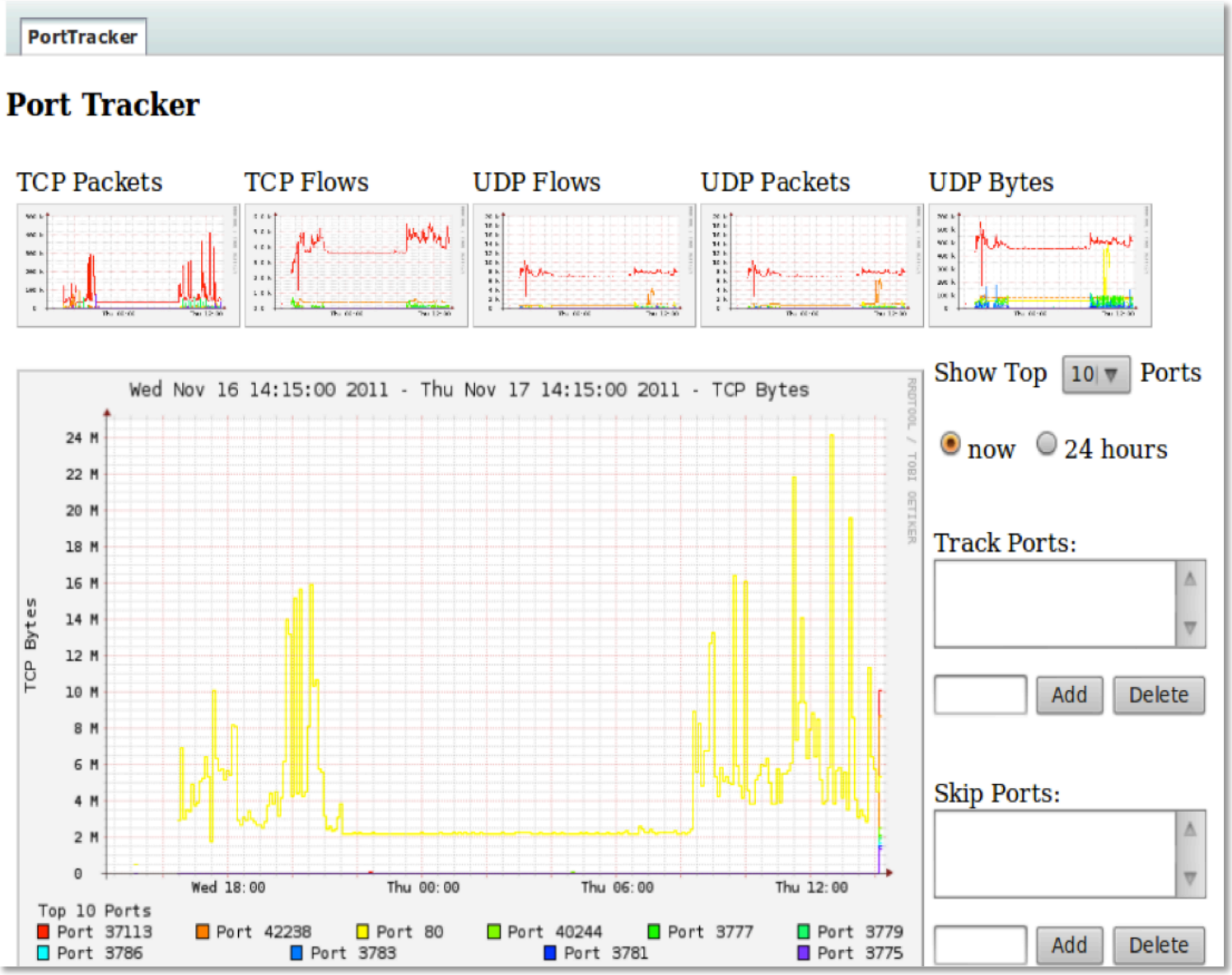
Plugins

Existen varios plugins:

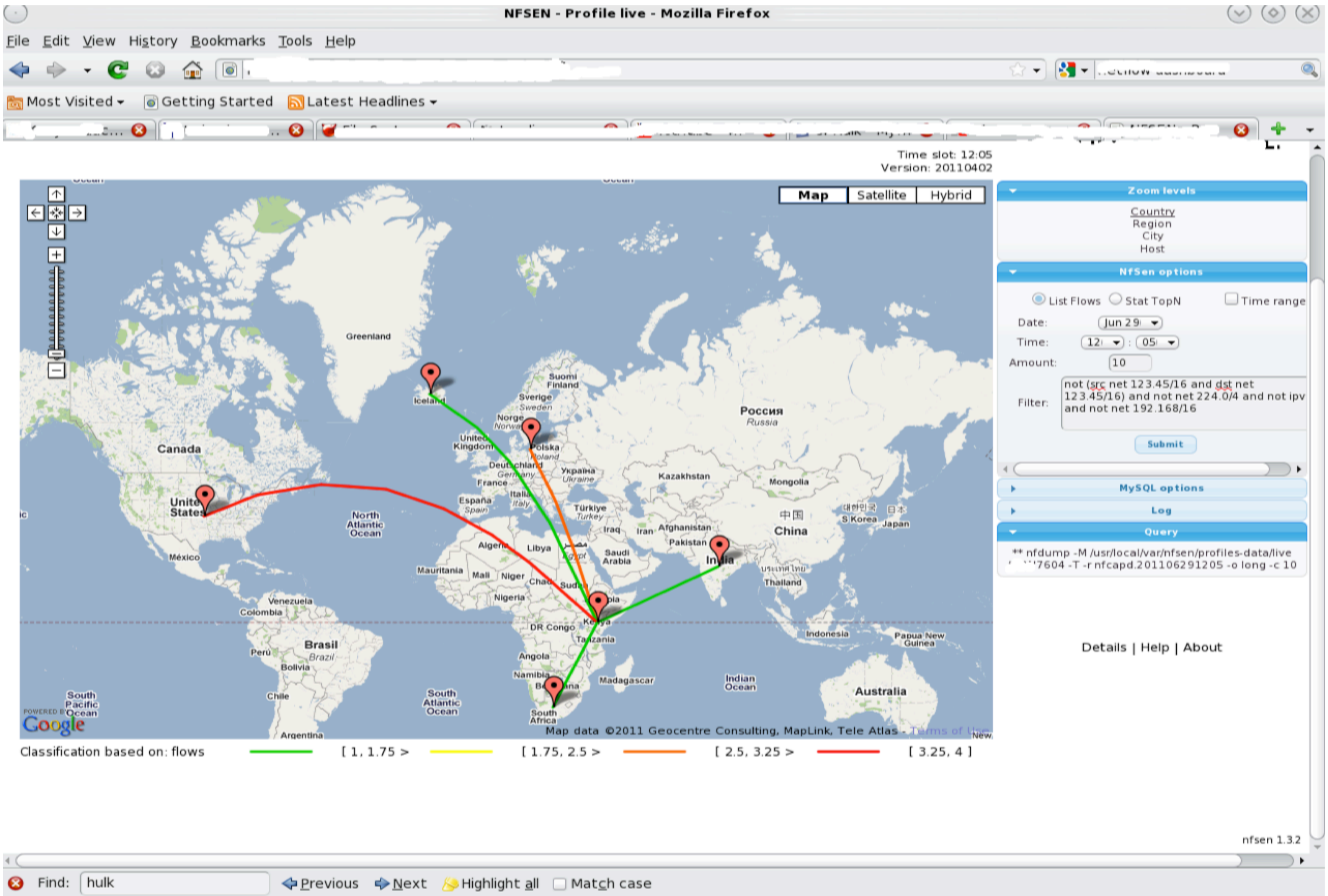
- **Portracker** muestra los 10 puertos más activos (top ten)
- **Surfmap** Muestra el tráfico en un mapa geográfico

Más plugins aquí
http://sourceforge.net/apps/trac/nfsen-plugins/

PortTracker



SurfMap



NFSEN - Profile live - Mozilla Firefox
File Edit View History Bookmarks Tools Help
Most Visited Getting Started Latest Headlines
Time slot: 12:05
Version: 20110402
Map Satellite Hybrid
Zoom levels
Country
Region
City
Host
NfSen options
List Flows Stat TopN Time range
Date: Jun 29
Time: 12 : 05
Amount: 10
Filter: not (src net 123.45/16 and dst net 123.45/16) and not net 224.0/4 and not ipv and not net 192.168/16
Submit
MySQL options
Log
Query
** nfdump -M /usr/local/var/nfsen/profiles-data/live ...7604 -T -r nfcapd.201106291205 -o long -c 10
Details | Help | About
Map data ©2011 Geocentre Consulting, MapLink, Tele Atlas
Classification based on: flows
[1, 1.75 >
[1.75, 2.5 >
[2.5, 3.25 >
[3.25, 4]
nfsen 1.3.2
Find: hulk
Previous Next Highlight all Match case

Cuando usar NfSen

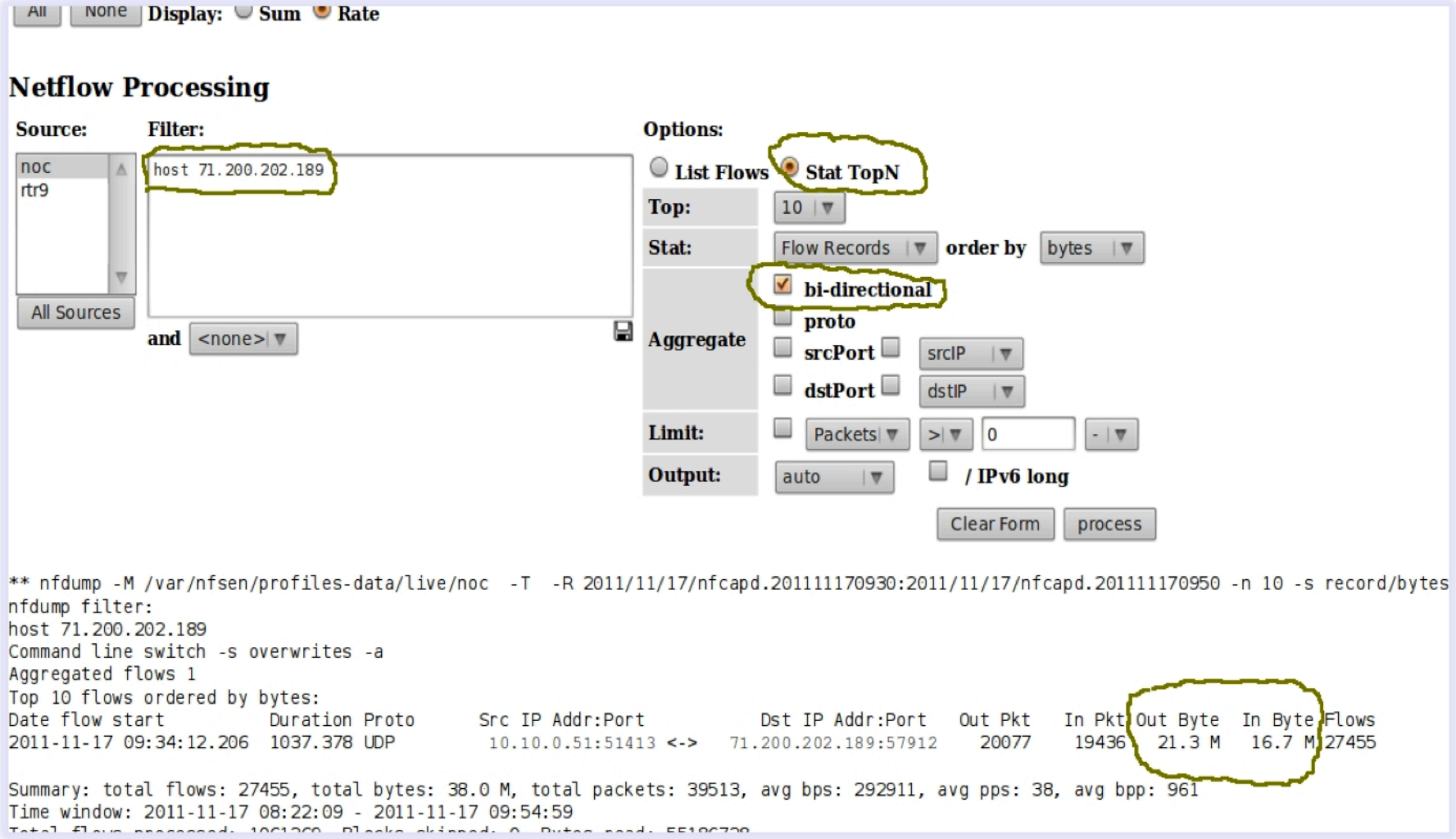
- Puede usarse para:
  - Investigación forense: qué tráfico y qué nodos estaban activos en un momento específico
  - Ver tráfico de entrada/salida entre AS, tráfico entre IPs o puertos origen/destino
  - Identificar los protocolos más usados
- Complementa a Cacti para ver información más detallada acerca del tipo de tráfico
- Con esta información se 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

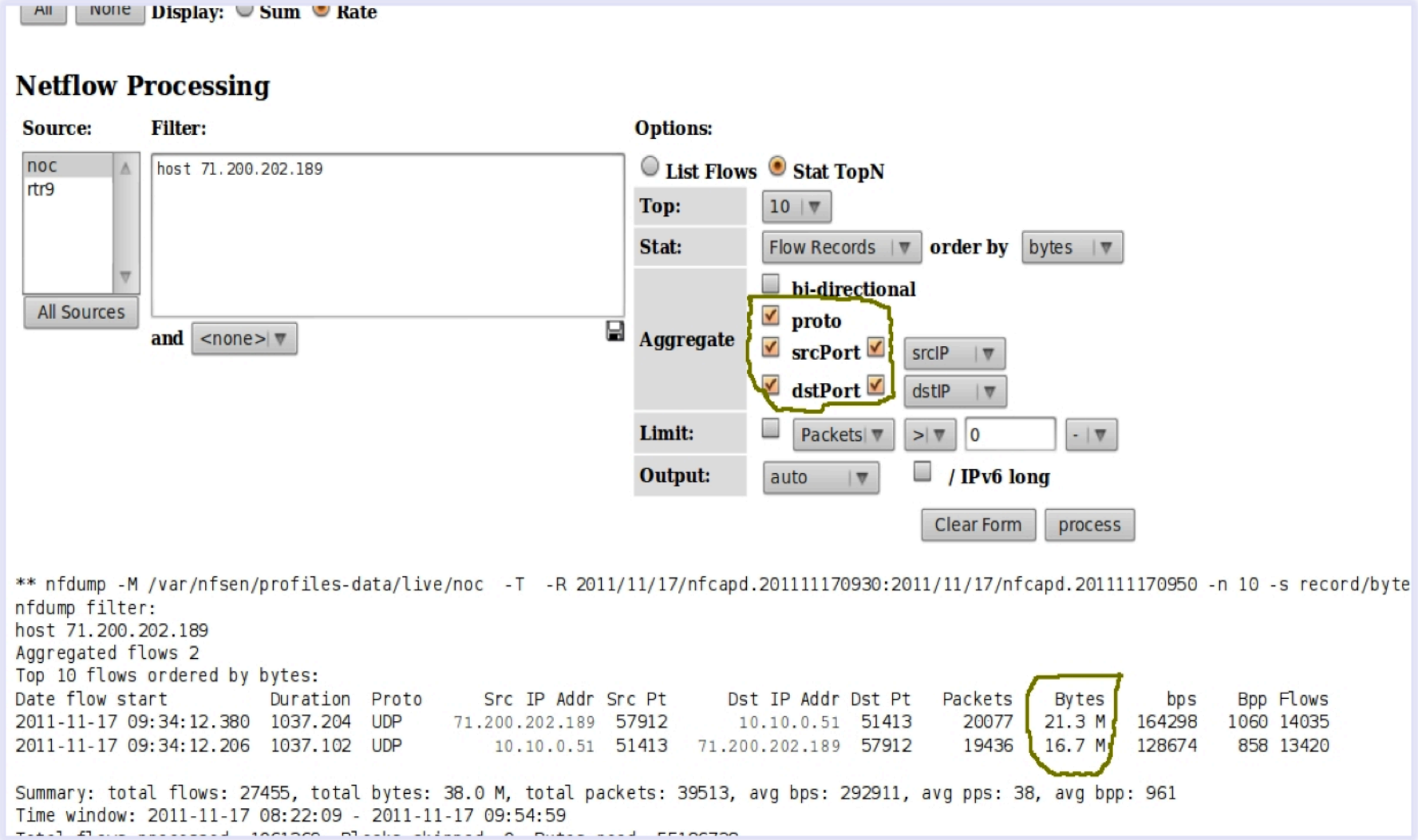
Unidireccional vs. Bidireccional

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

Bidireccional



Unidireccional



Referencias

NfSen

http://nfsen.sourceforge.net

NfDump

http://nfdump.sourceforge.net/

Ejercicios