Сетевое управление и мониторинг

NfSen

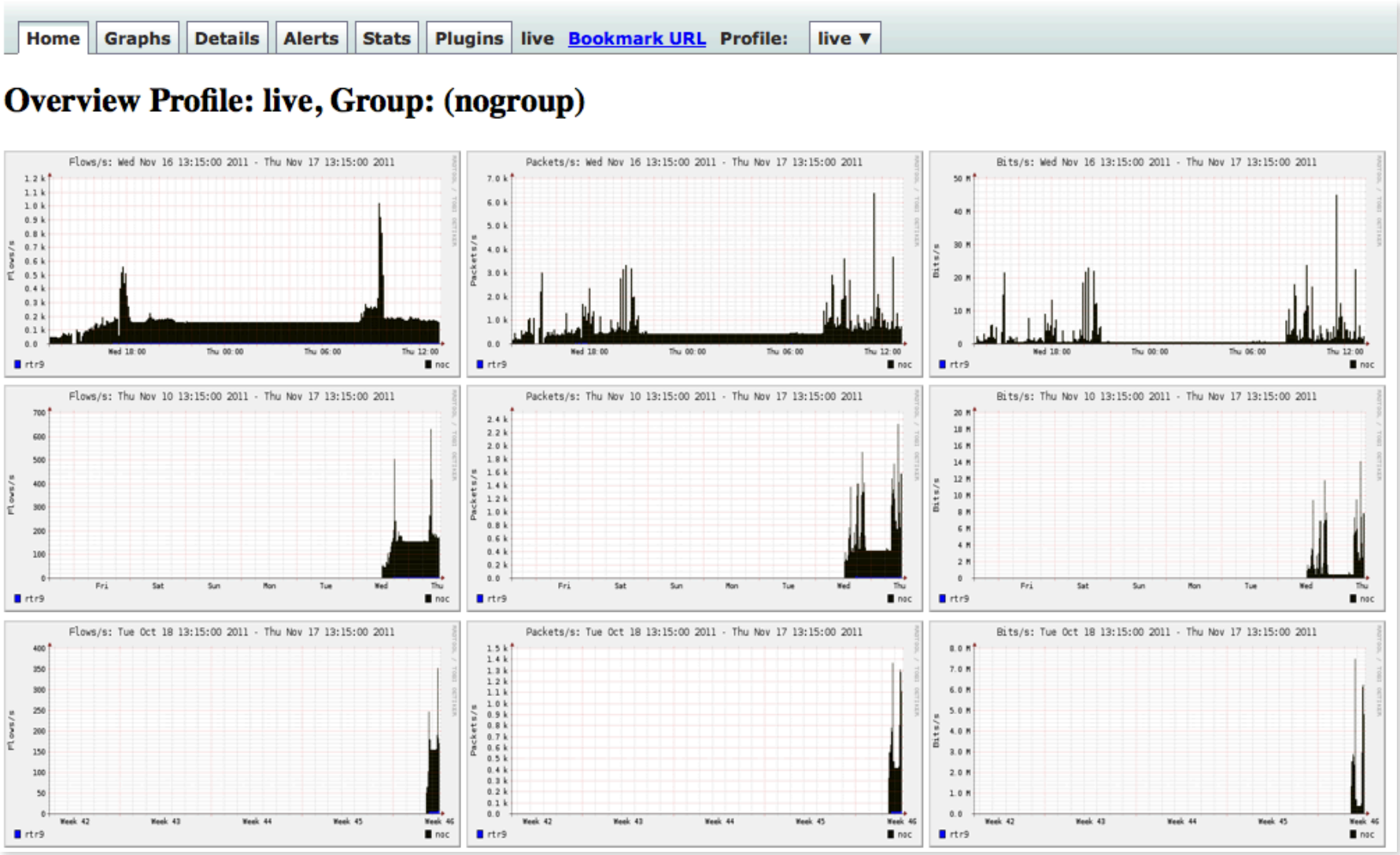
Что такое NfSen

- Это графический (Web) интерфейс к NfDump
- NfDump собирает и обрабатывает потоки netflow с командной строки
- NfSen позволяет:
  - Легко просматривать данные netflow.
  - Обрабатывать данные netflow, относящиеся к конкретному интервалу времени.
  - Создавать текущие профили и профили для истории
  - Создавать предупреждения, основываясь на различных условиях.
  - Создавать ваши собственные плагины для периодической обработки данных netflow.

Структура NfSen

- Файл конфигурации - nfsen.conf
- Файлы NfDump – файлы, содержащие собранные потоки – хранятся в каталоге ‘profiles-data’
  - NB: другие программы могут их читать, но не храните их слишком долго, потому что они могут переполнить диск
- Графики – хранятся в каталоге‘profiles-stat’

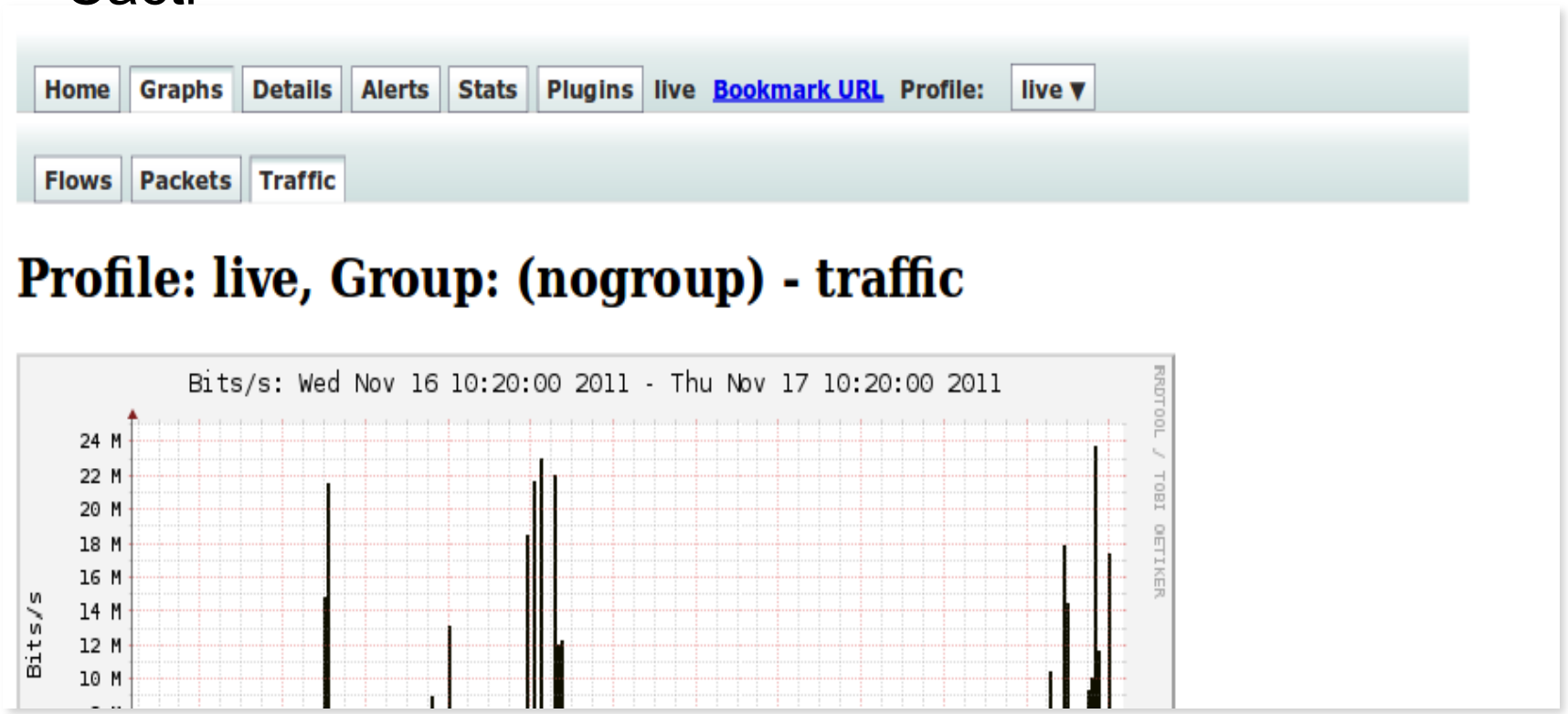
Главный экран NfSen



Вкладка “Graphs”

Графики потоков, пакетов, и трафика для интерфейсов с активированным сбором netflow

NB: То, что вы видите в графике “Traffic” должно быть очень похоже на график для того же интерфейса в Cacti



Страница “Details”

- Самая интересная страница
- Может показывать текущую либо сохраненную информацию о потоках
- Может показывать детальную информаци о Netflow, например:
  - Номера AS (интереснее, если на роутере есть полная таблица роутинга)
  - Хосты/порты источника, хосты/порты назначения
  - Однонаправленные либо двунаправленные потоки
  - Потоки на конкретном интерфейсе
  - Протоколы и TOS


Home
Graphs
Details
Alerts
Stats
Plugins
live
Bookmark URL
Profile:
live
Profile: live
TCP
UDP
ICMP
other
Wed Nov 16 22:25:00 2011 Bits/s any protocol
Bits/s any protocol
Wed 12:00
Wed 18:00
Thu 00:00
Thu 06:00
rtr9
noc
ProfileInfo:
Type: live
Max: unlimited
Exp: never
Start: Nov 16 2011 - 12:10 UTC
End: Nov 17 2011 - 10:25 UTC
t start 2011-11-16-22-25
t end 2011-11-16-22-25
Packets
Flows
Select
Single Timeslot
Display:
1 day
Lin Scale
Stacked Graph
Log Scale
Line Graph
Statistics timeslot Nov 16 2011 - 22:25
Channel:
Flows:
Packets:
Traffic:
all:
tcp:
udp:
icmp:
other:
noc
149.1 /s
29.3 /s
50.6 /s
69.2 /s
0 /s
393.2 /s
222.7 /s
52.2 /s
118.3 /s
0 /s
348.3 kb/s
226.4 kb/s
41.0 kb/s
80.9 kb/s
0 b/s
rtr9
5.1 /s
1.7 /s
3.0 /s
0.4 /s
0 /s
17.5 /s
8.6 /s
3.0 /s
6.0 /s
0 /s
13.7 kb/s
7.4 kb/s
2.2 kb/s
4.1 kb/s
0 b/s
All
None
Display:
Sum
Rate
Netflow Processing
Source:
Filter:
Options:
noc
rtr9
All Sources
List Flows
Stat TopN
Top:
10
Stat:
Any IP Address
order by
flows
Limit:
Packets
>
0
Output:
/ IPv6 long
and
<none>
Clear Form
process
Netflow traffic graphs organized by Protocol
Time period for flows being observed
Graph of Netflow traffic for all Protocols
Routers being monitored
Extended Netflow processing options

Предупреждения и статистика

Страница “Alerts”

- Может создавать предупреждения основанные на установленных пороговых значениях, например, увеличение либо уменьшение трафика
- Когда условие выполнена, может отправлять E-mail с предупреждением

Страница “Stats”

- Может создавать графики основанные на определенной информации
  - номера AS,
  - IP/порты источника/назначения
  - входящие/выходящие интерфейсы
  - и другие

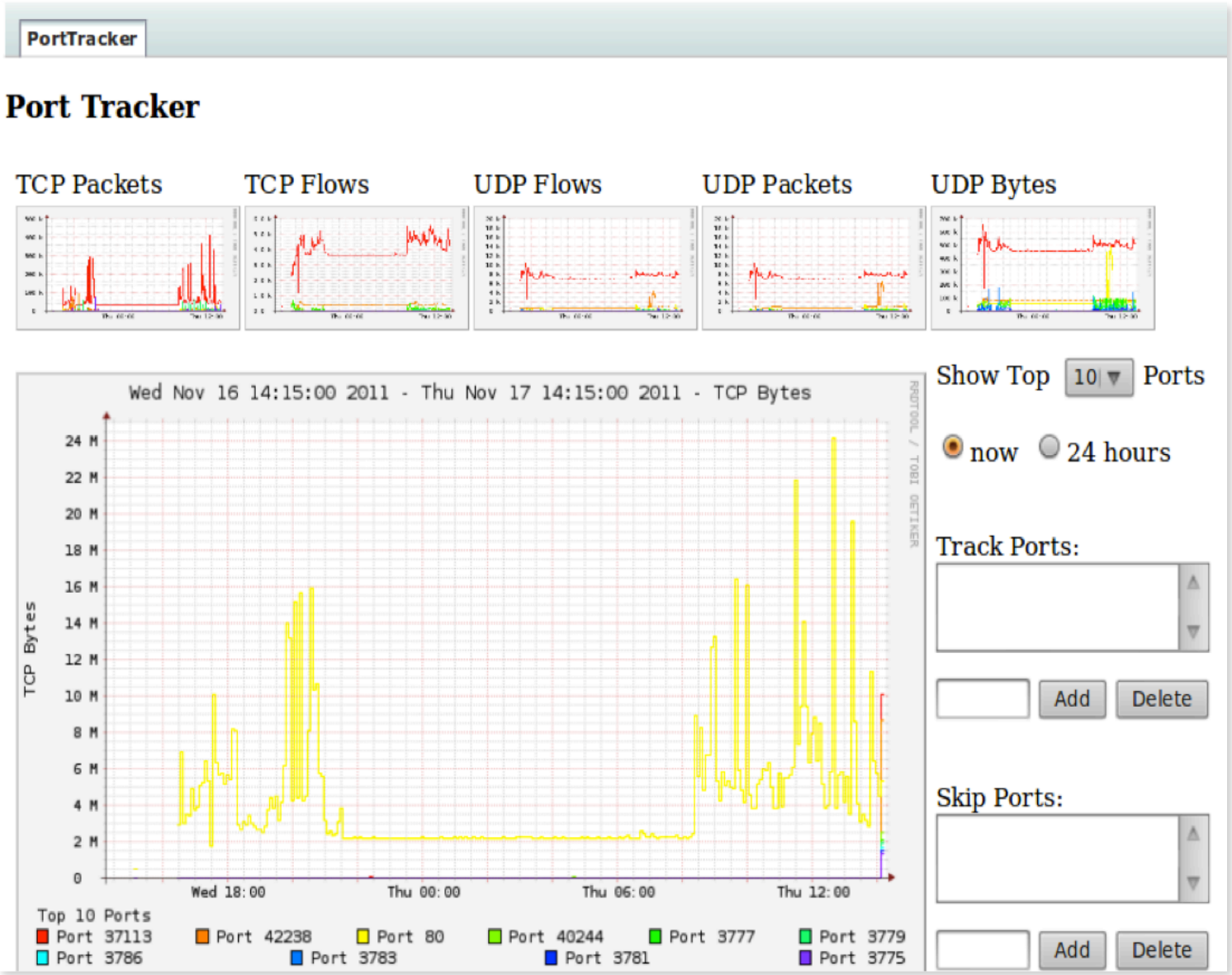
Плагины

Несколько доступных плагинов:

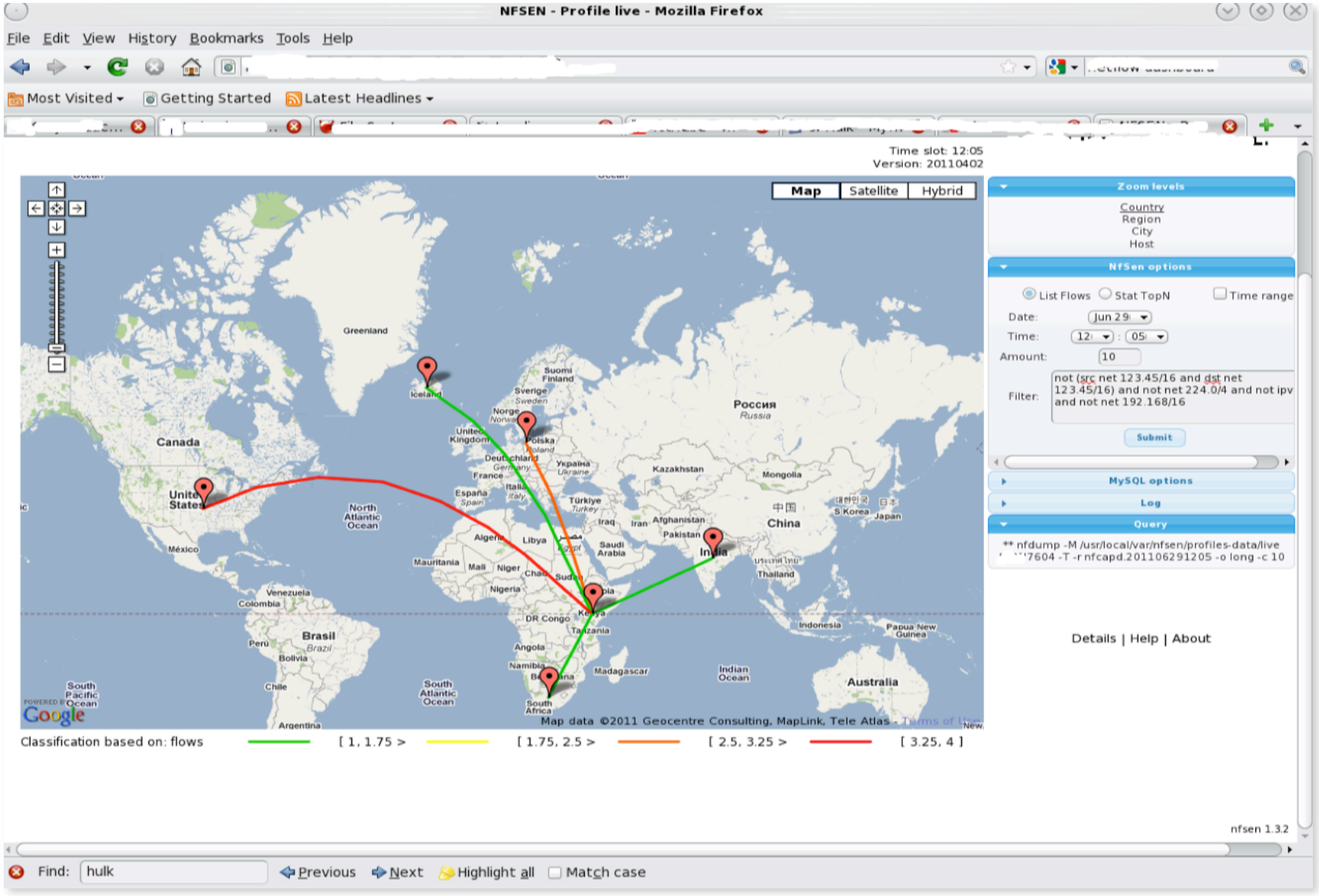
- **Portracker** отслеживает 10 наиболее активных портов и отображает их на графике
- **Surfmap** показывает трафик по странам, основываясь на определении страны по IP

Больше плагинов тут

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:
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
Greenland
Canada
Россия
Russia
China
India
Australia
Brasil
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

Когда использвать NfSen

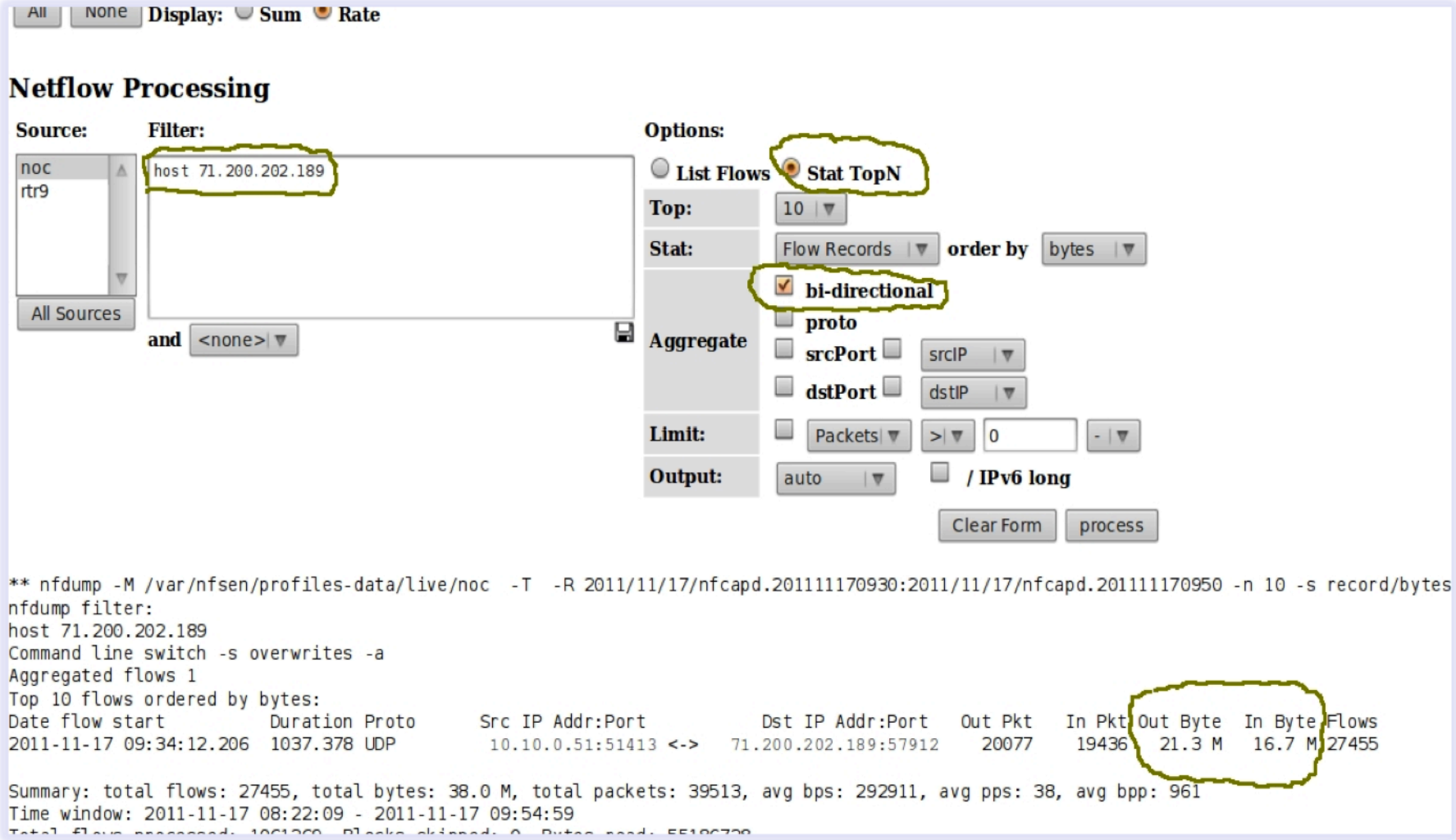
- Может использоваться для:
  - Расследований: какие хосты были активны в конкретное время
  - Просмотра трафика по номеру AS, по IP, по порту отправителя/получателя и другим параметрам
  - Определения наиболее активных IP или протоколов
- Может дополнять Cacti для получения более детальной информации о трафике
- Помогает находить проблемы и принимать информированные решения, например:
  - У вас большое количество трафика SMTP -> наверное есть зараженные машины посылающие спам
  - 80% вашего трафика идет на AS номер X. Возможно, есть смысл соединиться напрямую с этой сетью – дешевле выйдет

Двунаправленный и однонаправленный трафик, как его показывает NfSen

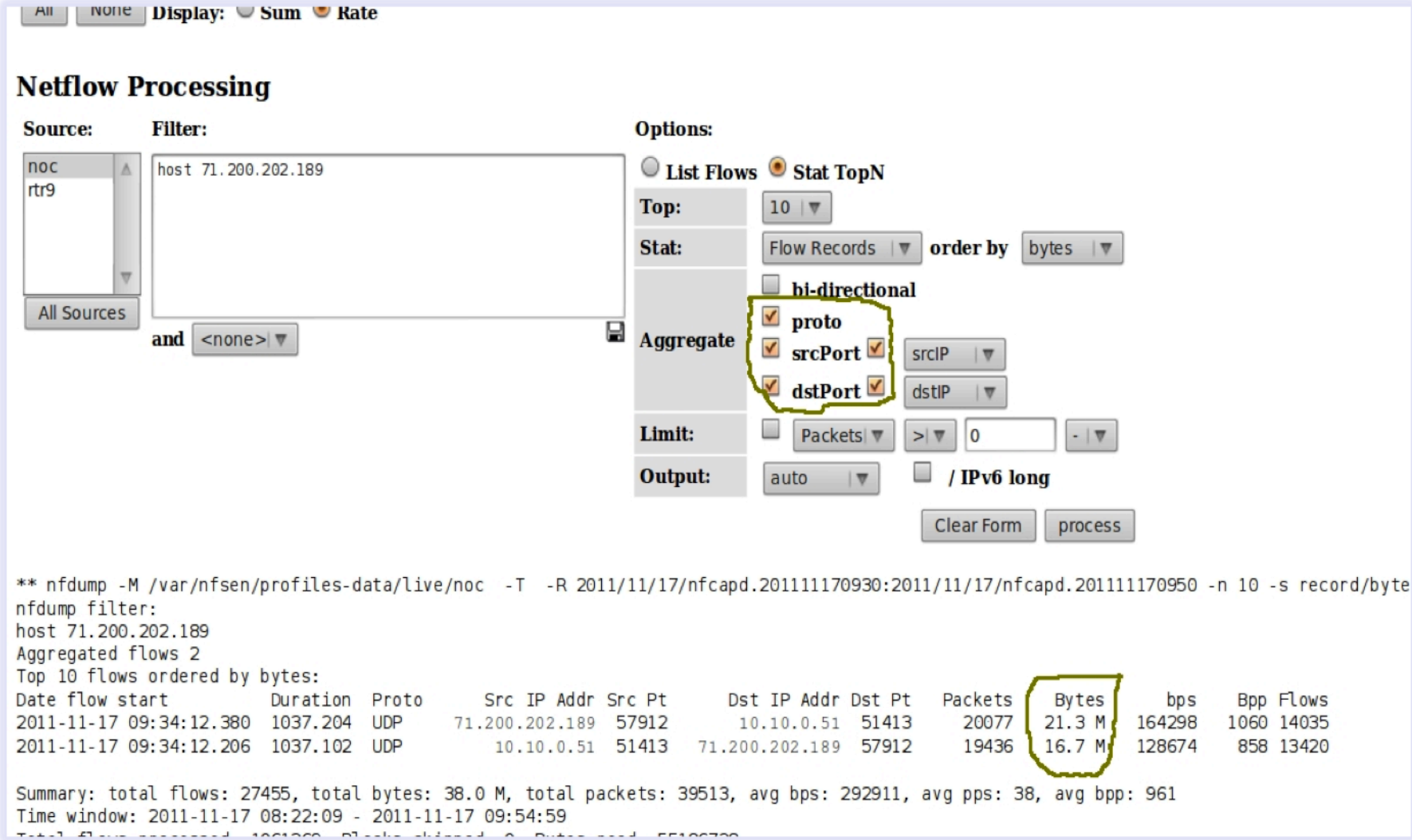
Однонаправленный и двунаправленный

- Однонаправленные потоки разделяют трафик от A к B от трафика от B к A
- Двунаправленные потоки объединяют трафик от A к B с трафиком от B к A
- Можно использовать с любыми другими фильтрами (порт отправитель, IP отправителя и т.д.)
- Список фильтров:
  - http://nfsen.sourceforge.net/#mozTocId652064

Двунаправленный



Однонаправленный



Ссылки

NfSen

http://nfsen.sourceforge.net

NfDump

http://nfdump.sourceforge.net/

Упражнения