



# Сетевое управление и МОНИТОРИНГ

NfSen



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

# 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.

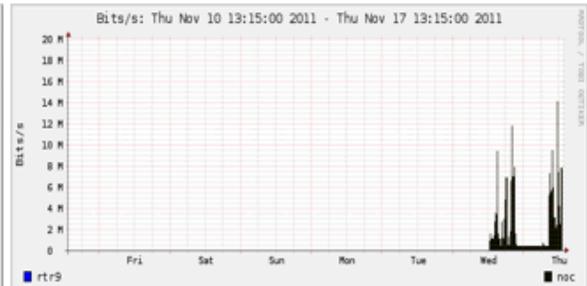
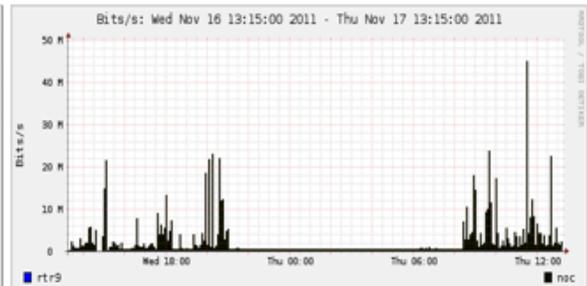
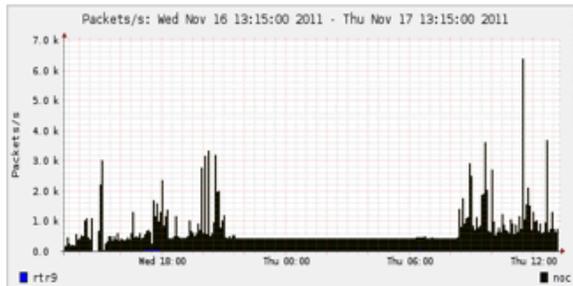
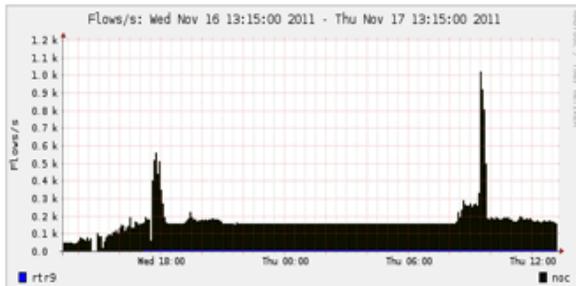
# Структура NfSen

- 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

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

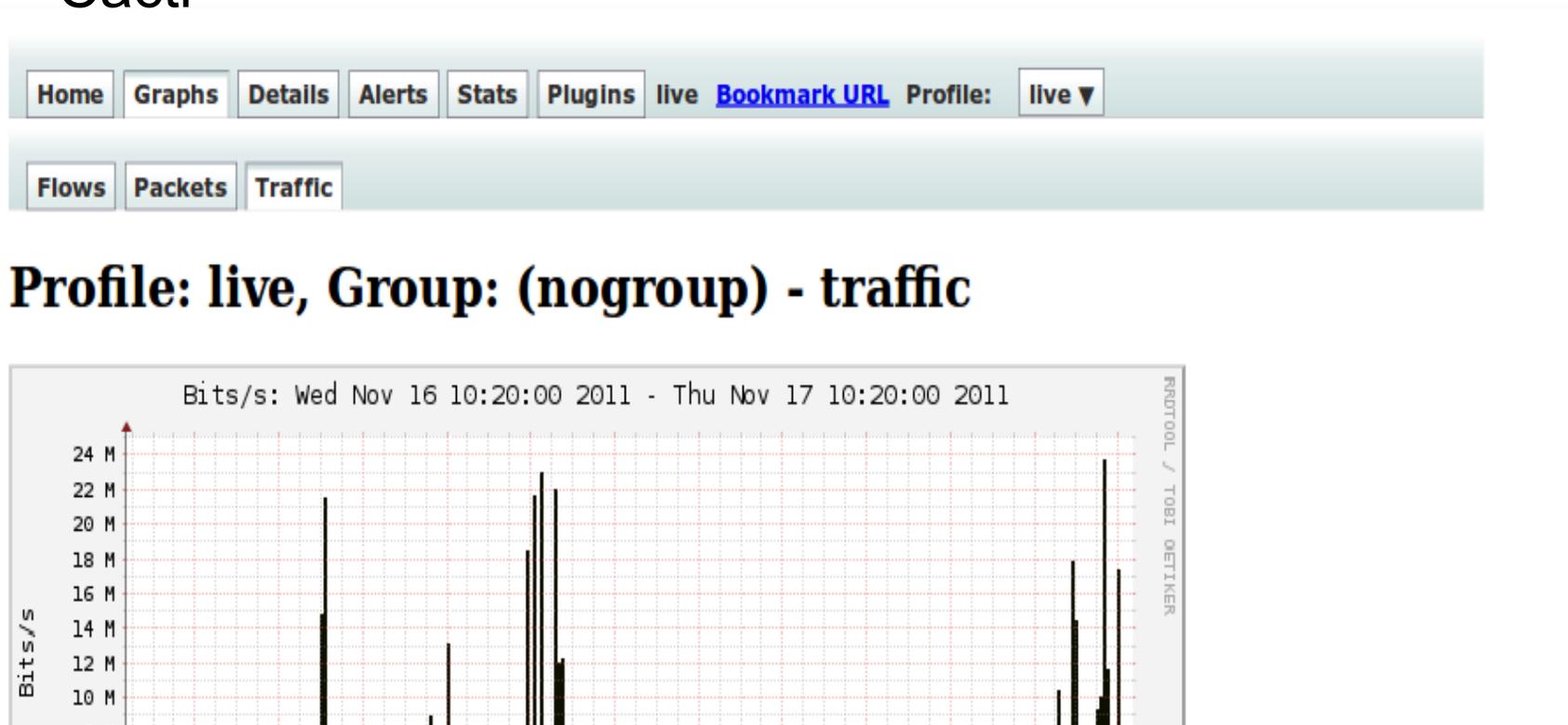
## Overview Profile: live, Group: (nogroup)



# 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 Sacti



# Страница “Details”

- Самая интересная страница
- Может показывать текущую либо сохраненную информацию о потоках
- Может показывать детальную информации 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

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

Lin Scale  Stacked Graph  
 Log Scale  Line Graph

Select Single Timeslot Display: 1 day

### Statistics timeslot Nov 16 2011 - 22:25

Channel:	Flows:					Packets:					Traffic:				
	all:	tcp:	udp:	icmp:	other:	all:	tcp:	udp:	icmp:	other:	all:	tcp:	udp:	icmp:	other:
<input checked="" type="checkbox"/> 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
<input checked="" type="checkbox"/> 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: noc rtr9 All Sources

Filter: and <none>

Options:  
 List Flows  Stat TopN  
 Top: 10  
 Stat: Any IP Address order by flows  
 Limit: Packets > 0  
 Output: / IPv6 long

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

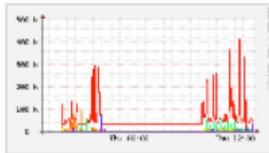
Больше плагинов тут

# PortTracker

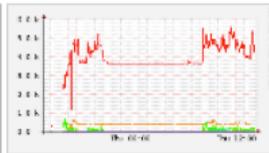
PortTracker

## Port Tracker

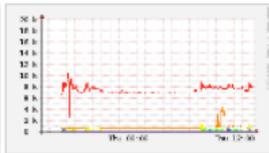
TCP Packets



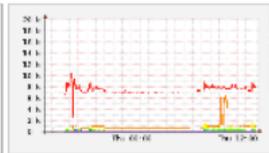
TCP Flows



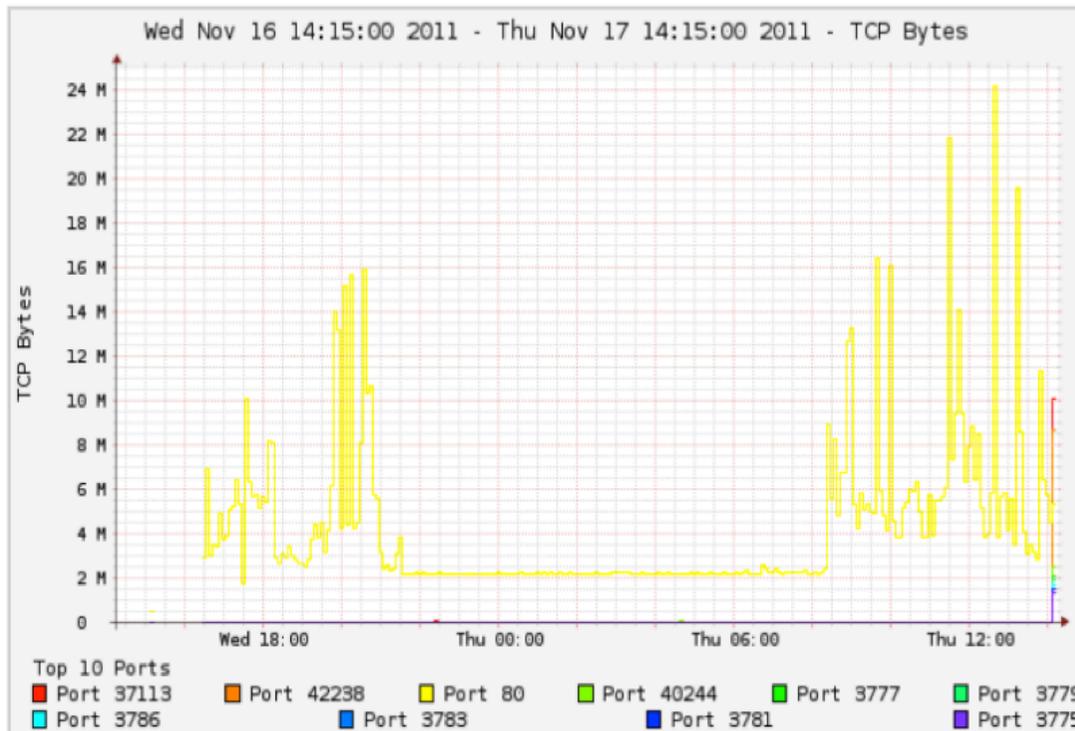
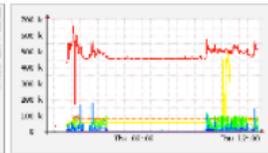
UDP Flows



UDP Packets



UDP Bytes



Show Top 10 Ports

now  24 hours

Track Ports:

Add Delete

Skip Ports:

Add Delete

# SurfMap

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

Classification based on: flows [ 1, 1.75 > [ 1.75, 2.5 > [ 2.5, 3.25 > [ 3.25, 4 ]

Map data ©2011 Geocentre Consulting, MapLink, Tele Atlas - Terms of Use

nfsen 1.3.2

Find: hulk Previous Next Highlight all Match case

# Когда использовать 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 Sacti 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 А к В от трафика от В к А
- Двунаправленные потоки объединяют трафик от А к В с трафиком от В к А
- Можно использовать с любыми другими фильтрами (порт отправитель, IP отправителя и т.д.)
- Список фильтров:
  - <http://nfsen.sourceforge.net/#mozTocId652064>

# Двунаправленный

All None Display:  Sum  Rate

## Netflow Processing

Source: noc  
rtr9

Filter: host 71.200.202.189

Options:  List Flows  Stat TopN

Top: 10

Stat: Flow Records order by bytes

bi-directional

Aggregate

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: 1861360, flows skipped: 0, bytes read: 55186728
```

# Однонаправленный

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
```

# Ссылки

NfSen

<http://nfsen.sourceforge.net>

NfDump

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



# Упражнения