Gestion et supervision des Réseaux

NfSen

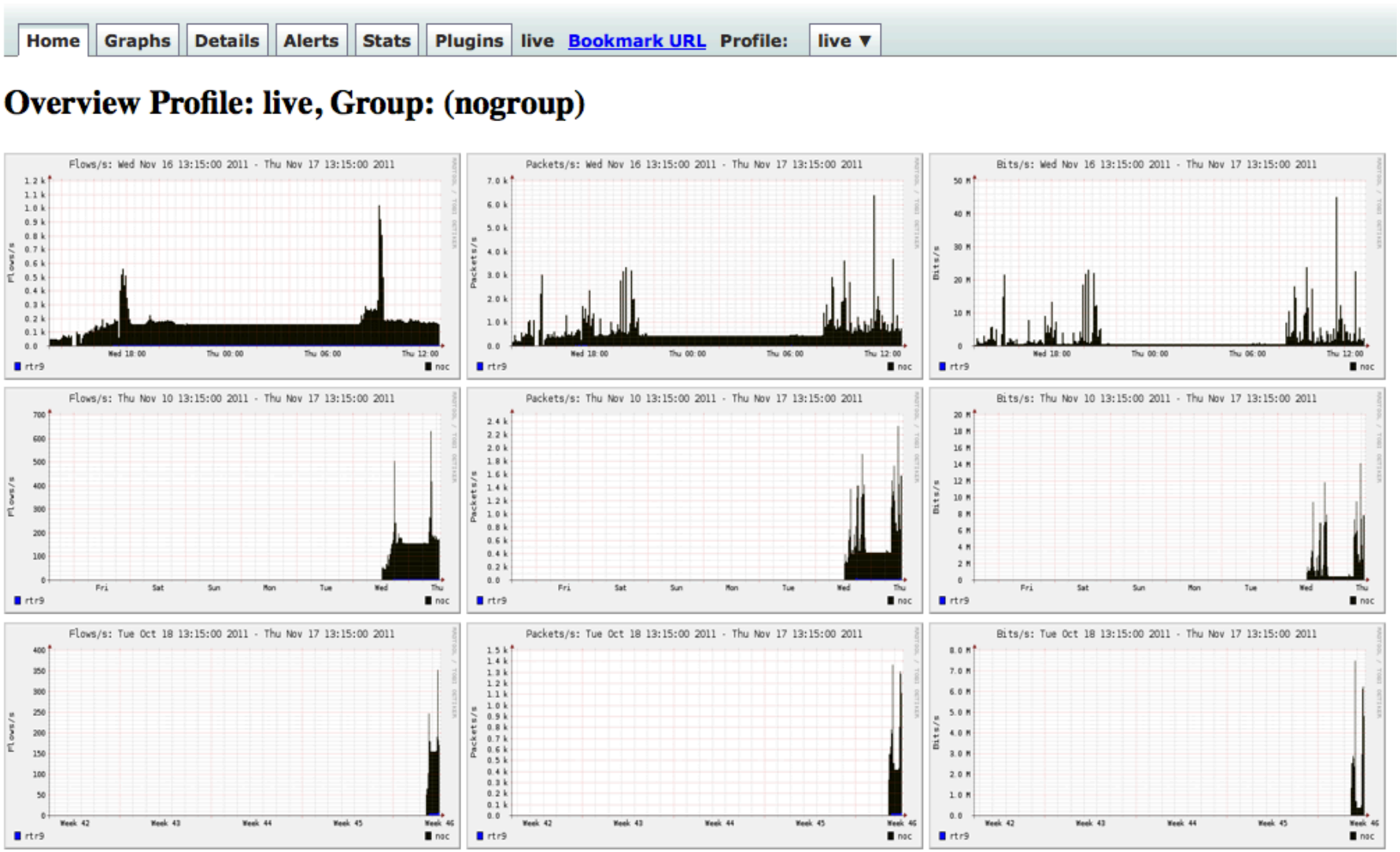
Qu’est-ce que NfSen

- Un outil graphique (Web) qui sert d’interface à NfDump
- Les NfDump outils collectent et traitent les données netflow au niveau de la CLI
- NfSEN permet:
  - Naviguer facilement dans les flux NetFlow
  - Analyser les données netflow dans un intervalle de temps donné
  - Créer un historique ainsi que des profils d’analyse
  - Régler des alertes, en fonction des conditions
  - Écrire vos propres extensions pour traiter les données à intervalles réguliers.

Structure de NfSen

- Fichier de configuration – nfsen.conf
- Fichier de collecte nfdump – des fichiers contenant des flux collectés et stockés dans un répertoire ‘profiles-data’
  - NB: Ne pas laisser les fichiers Nfdump trop longtemps sur le disque, ceux-vi peuvent remplir le système de fichier!
- Les graphiques eux-même sont stockés dans un répertoire ‘profiles-stat’

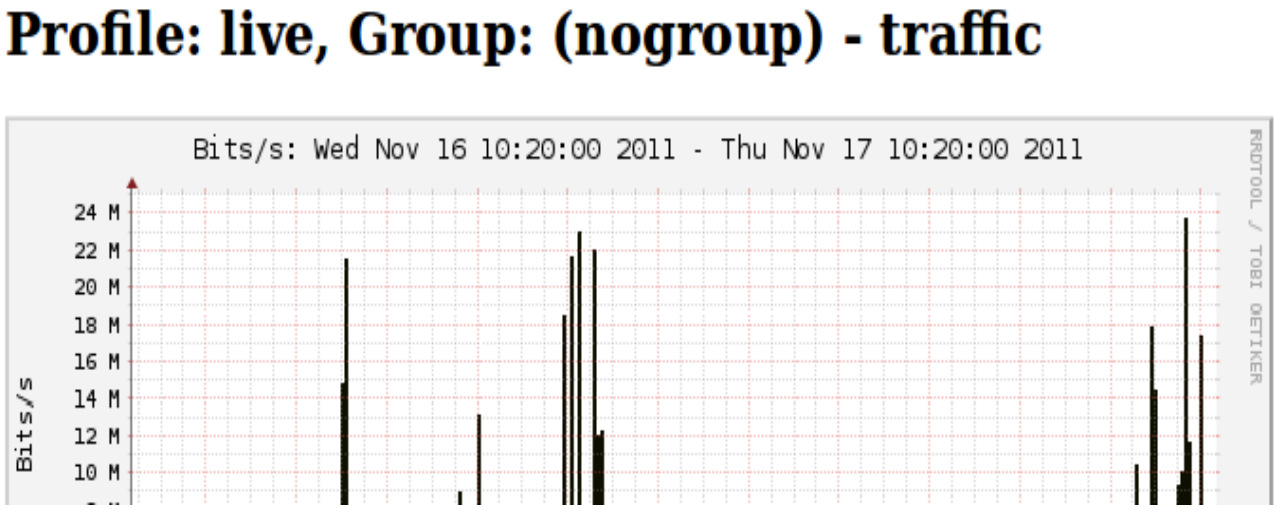
Écran d'accueil NfSen



Onglet “Graphs”

Graphes des flux, paquets et du traffic, issus de l’interface sur laquelle netflow est activé

NB: En principe ce que vous voyez sous Traffic doit correspondre au traffic Cacti pour la même interface



Page Détails

- La page la plus intéressante
- Pour visualiser les informations NetFlow courantes ou bien les infos stockées
- Visualiser des infos Netflow telles que:
  - Numéro d'AS Numbers (utile si vous avez une table de routage complet exportée sur votre routeur)
  - Machine, port source, machine, port dest.
  - Flux uni- ou bi-directionnels
  - Flux sur des interfaces particulières
  - Protocoles et 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
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
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
and
<none>
List Flows
Stat TopN
Top:
10
Stat:
Any IP Address
order by
flows
Limit:
Packets
>
0
Output:
/ IPv6 long
Clear Form
process
Trafic netflow, graphes triés par protocole
Graphes NetFlow pour les protocoles
Période pour l'échantillon selectionné ou la vue entière
Les routeurs surveillés
Options de traitement Netflow avancées

Alertes et statistiques

Page d'alerte

- Créer des alertes en fonction de seuils définis, ex: montée ou baisse du traffic.
- On peut envoyer un mail en cas d'alerte

Page de stats

- Création de graphiques en fonction de critères précis.
  - ASNs,
  - Machine/ IP destination / Ports
  - Interfaces entrée / sortie
  - Et d'autres…

Extensions

Plusieurs extensions disponibles

- **Portracker** suivi des 10 protocoles les plus utilisés et création d'un graphe
- **Surfmap** affichage d'une carte de pays basée sur une base de géolocation

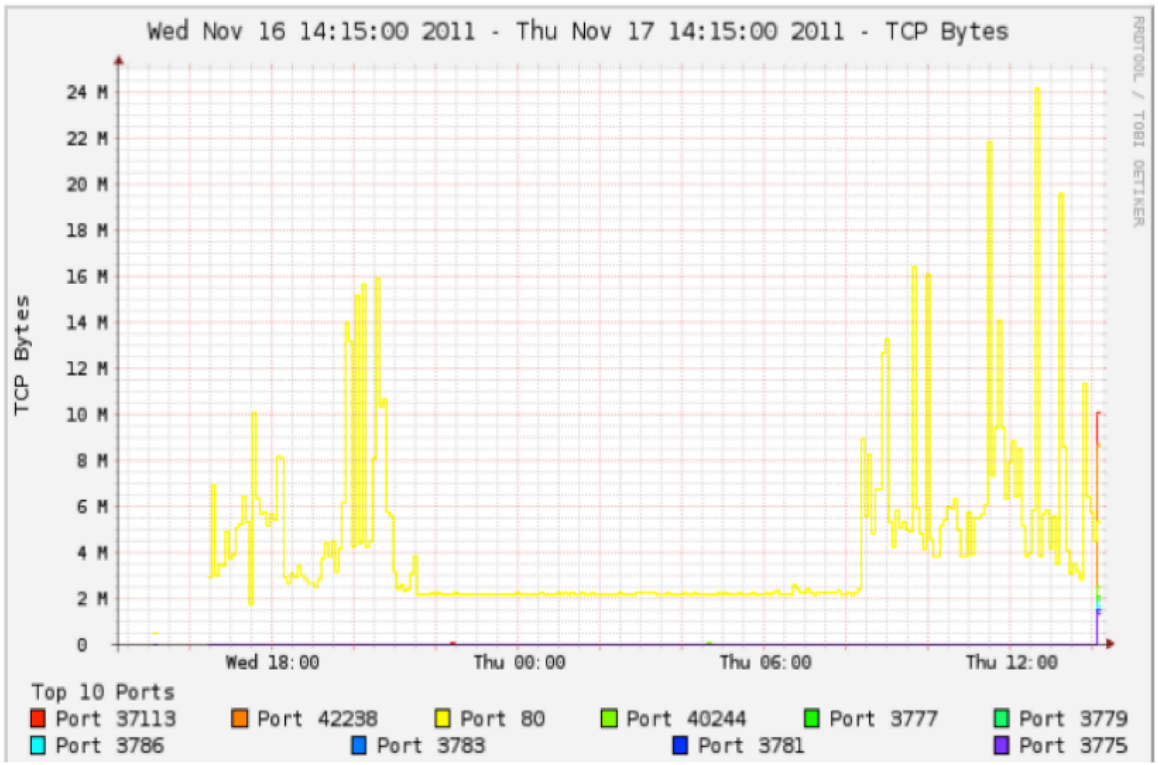
D'autres extensions:
http://sourceforge.net/apps/trac/nfsen-plugins/

PortTracker

PortTracker

Port Tracker

TCP Packets | TCP Flows | UDP Flows | UDP Packets | UDP Bytes



Show Top 10 Ports

now 24 hours

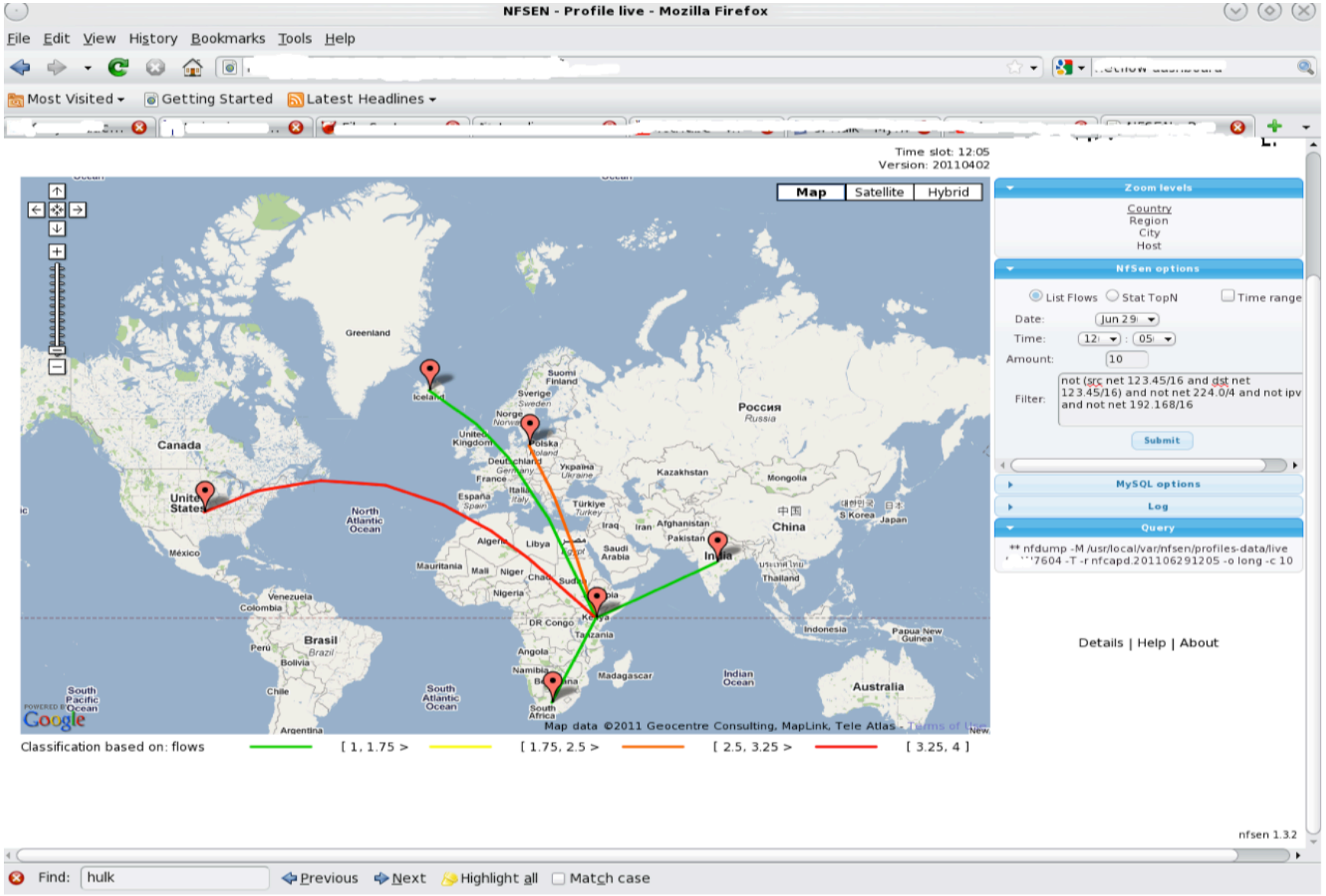
Track Ports:

Add Delete

Skip Ports:

Add Delete

SurfMap


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
nfsen 1.3.2
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]
Find: hulk
Previous
Next
Highlight all
Match case

Quand utiliser NFSen

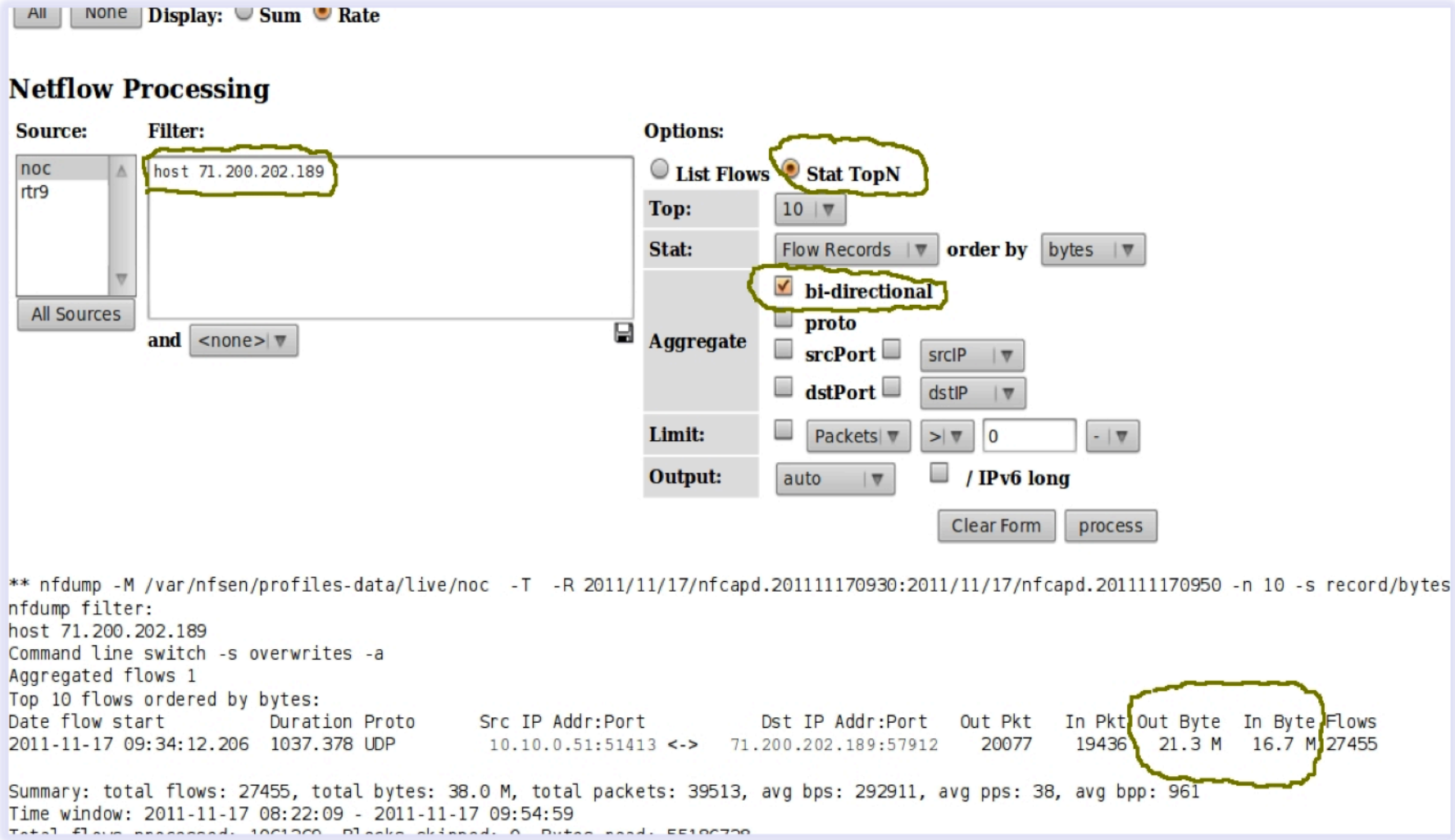
- Peut être utilisé pour:
  - Travail légiste: quelles machines actives à quel moment
  - Visualiser le traffic par AS src/dst, port/IP src/dst, et bien d'autres options
  - Identification des protocoles et IP les plus actifs
- C'est un outil qui complémente Cacti pour que vous ayez une vue plus détaillée du trafic
- Avec ces informations, vous pouvez prendre des décisions telles que:
  - Beaucoup de trafic SMTP ? Des machines peuvent être en train d'envoyer du SPAM/ sont infectées
  - 80% de votre trafic va vers l'AS X. Pourquoi ne pas interconnecter directement avec eux pour économiser ?

Trafic uni- et bi-directionnel tel que vu par NfSen

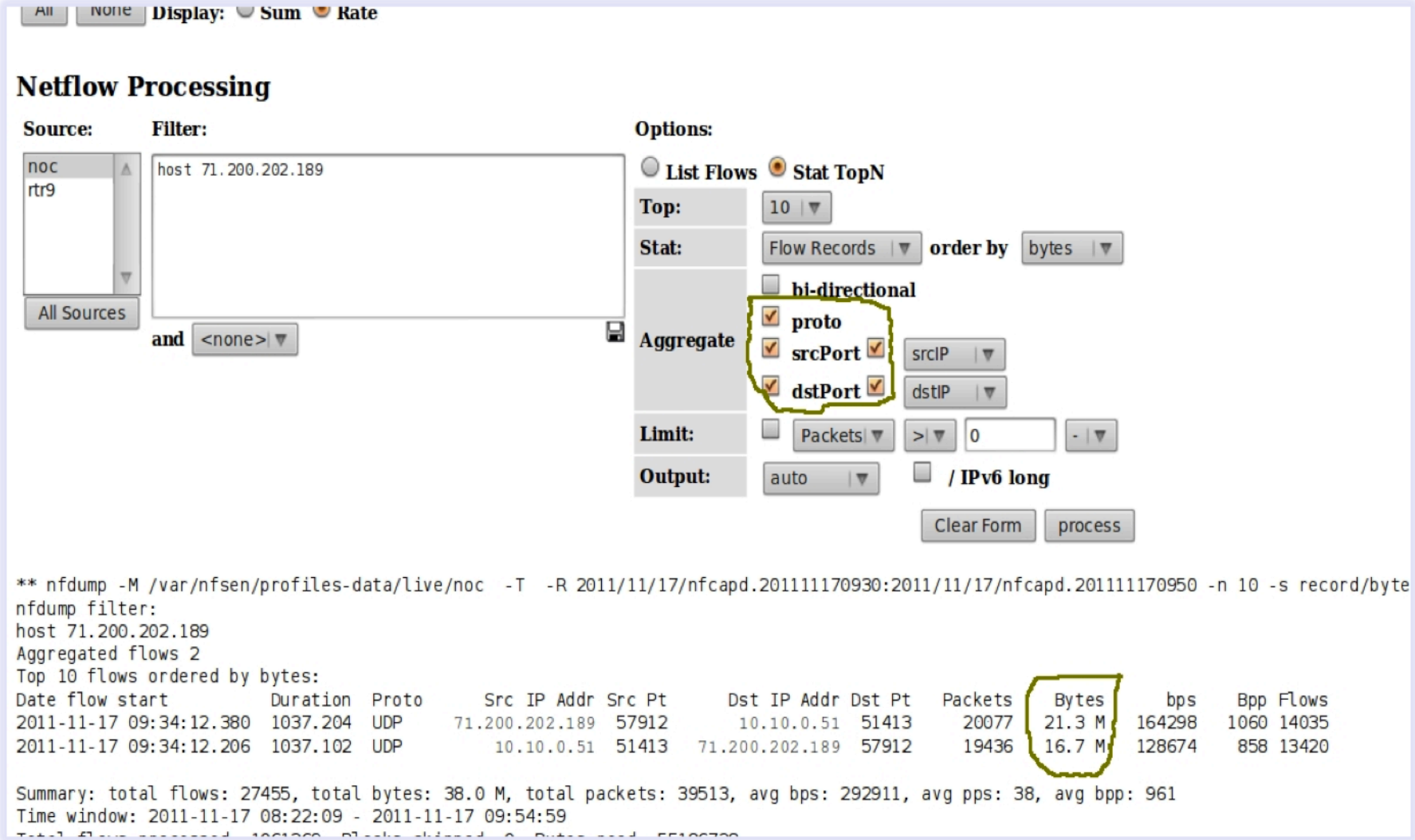
Unidirectionnel et Bidirectionnel

- Unidirectionnel: un flux A -> B, et un B -> A
- Bidirectionnel: des flux entre A <-> B
- À combiner avec d'autres filtres (port src, machines source, etc…)
- La liste des filtres est disponible ici
  - http://nfsen.sourceforge.net/#mozTocId652064

Bidirectionnel



Unidirectionel



Références

NFSEN

http://nfsen.sourceforge.net

NFDUMP

http://nfdump.sourceforge.net/

Exercices