



Gestion et supervision des Réseaux

NfSen



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

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.

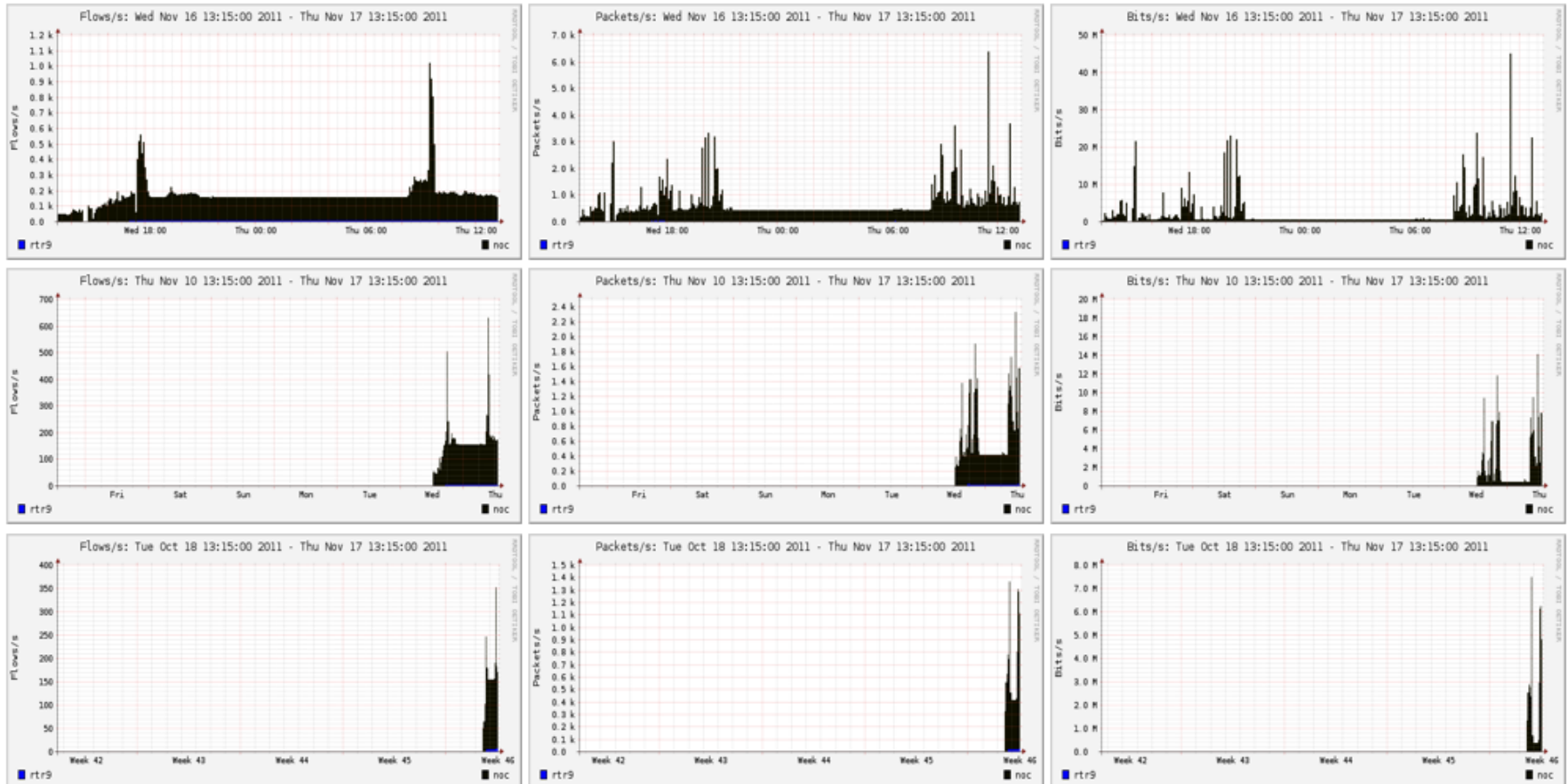
Structure de NfSen

- 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-ci peuvent remplir le système de fichier!
- Les graphiques eux-même sont stockés dans un répertoire 'profiles-stat'

Écran d'accueil NfSen

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

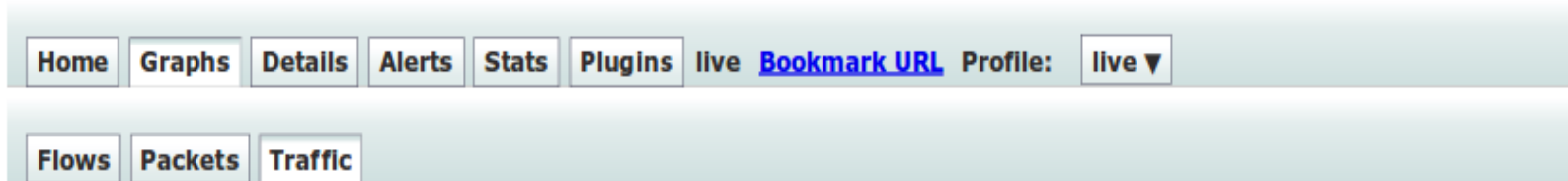
Overview Profile: live, Group: (nogroup)



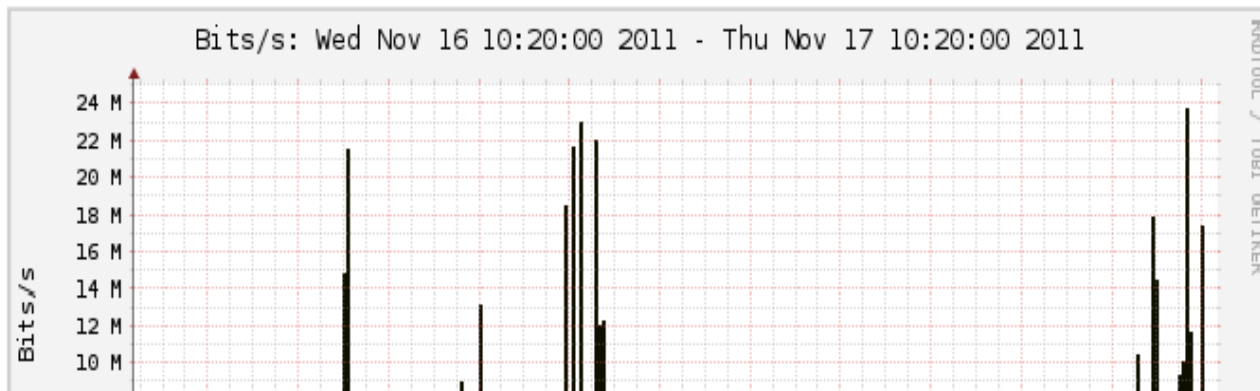
Onglet “Graphs”

Graphes des flux, paquets et du trafic, 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



Profile: live, Group: (nogroup) - traffic

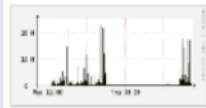


Page Détails

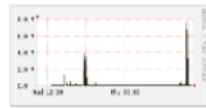
- La page la plus intéressante
- Pour visualiser les informations NetFlow courantes ou bien les infos stockées
- Visualiser des infos Netflow telles que:
 - Numéro d'AS Numbers (utile si vous avez une table de routage complet exportée sur votre routeur)
 - Machine, port source, machine, port dest.
 - Flux uni- ou bi-directionnels
 - Flux sur des interfaces particulières
 - Protocoles et ToS

Profile: live

TCP



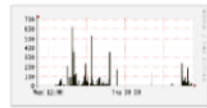
UDP



ICMP



other



Trafic netflow,
graphes triés par
protocole

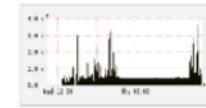
ProfileInfo:

Type: live
Max: unlimited
Exp: never
Start: Nov 16 2011 - 12:10 UTC
End: Nov 17 2011 - 10:25 UTC

tstart 2011-11-16-22-25

tend 2011-11-16-22-25

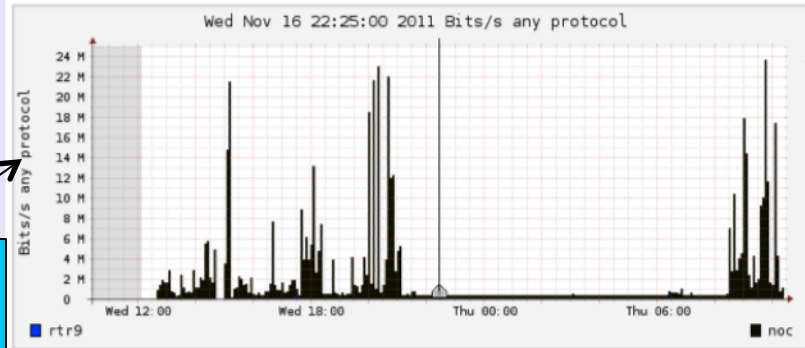
Packets



Flows



Période pour
l'échantillon
selectionné ou
la vue entière



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:	all:	tcp:	udp:	icmp:	other:	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:

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

Options de
traitement Netflow
avancées

Clear Form process

Graphes
NetFlow
pour les
protocoles

Les
routeurs
surveillés

Alertes et statistiques

Page d'alerte

- Créer des alertes en fonction de seuils définis, ex: montée ou baisse du trafic.
- 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 géolocalisation

D'autres extensions:

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

PortTracker

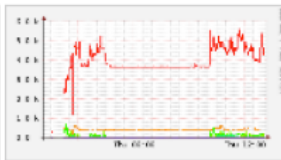
PortTracker

Port Tracker

TCP Packets



TCP Flows



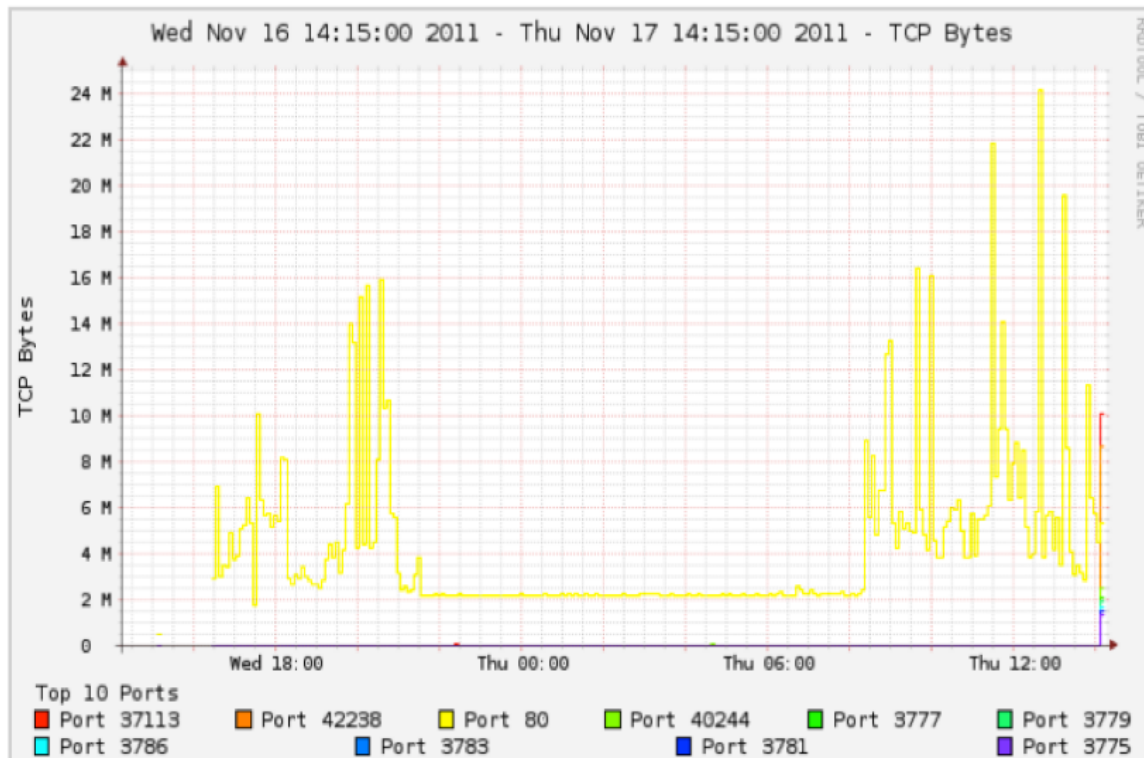
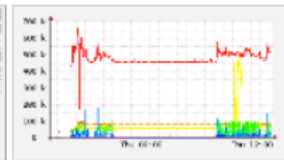
UDP Flows



UDP Packets



UDP Bytes



Show Top 10 Ports

☒ now ☐ 24 hours

Track Ports:

Add Delete

Skip Ports:

Add Delete

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

nfsen 1.3.2

Quand utiliser NFSen

- Peut être utilisé pour:
 - Travail légiste: quelles machines actives à quel moment
 - Visualiser le trafic 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 complète 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 $A \rightarrow B$, et un $B \rightarrow A$
- Bidirectionnel: des flux entre $A \leftrightarrow B$
- À combiner avec d'autres filtres (port src, machines source, etc...)
- La liste des filtres est disponible ici
 - <http://nfsen.sourceforge.net/#mozTocId652064>

Bidirectionnel

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: 1061360, Blocks skipped: 0, Bytes read: 55186738
```

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: 1061260, flows skipped: 0, bytes read: 55186700
```

Références

NFSEN

<http://nfsen.sourceforge.net>

NFDUMP

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

Exercices