Utilisation de NfSen

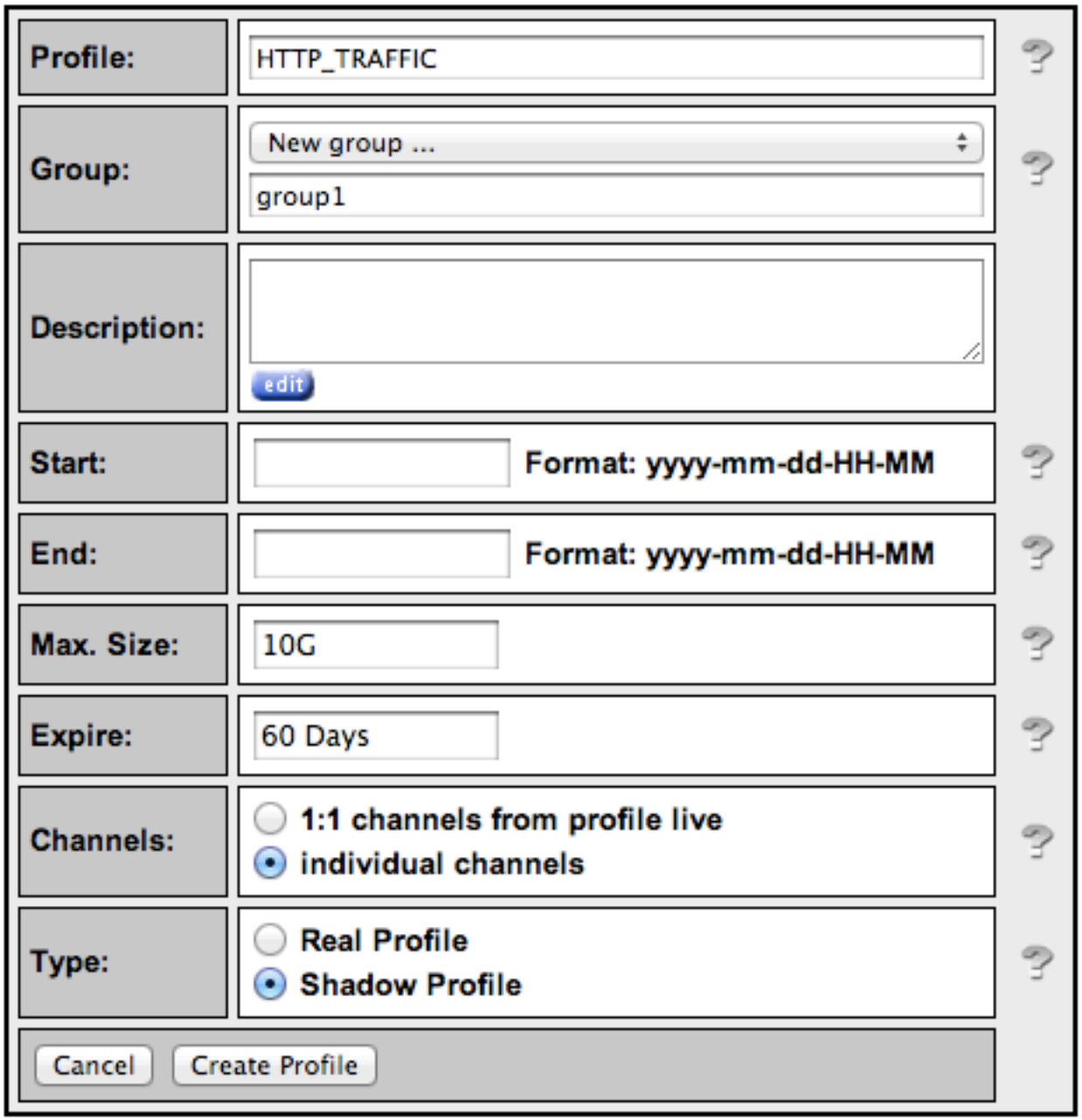
Ce qu'on va faire

1. Votre routeur doit être en train d'envoyer des flux vers un PC dans votre groupe, et un PC dans le groupe voisin. Vérifier!
2. S'assurer que NfSen fonctionne en navigant sur la page et vérifier que les graphes fonctionnent sans erreur
3. Nous allons maintenant voir quel type de traffic traverse ces deux routeurs

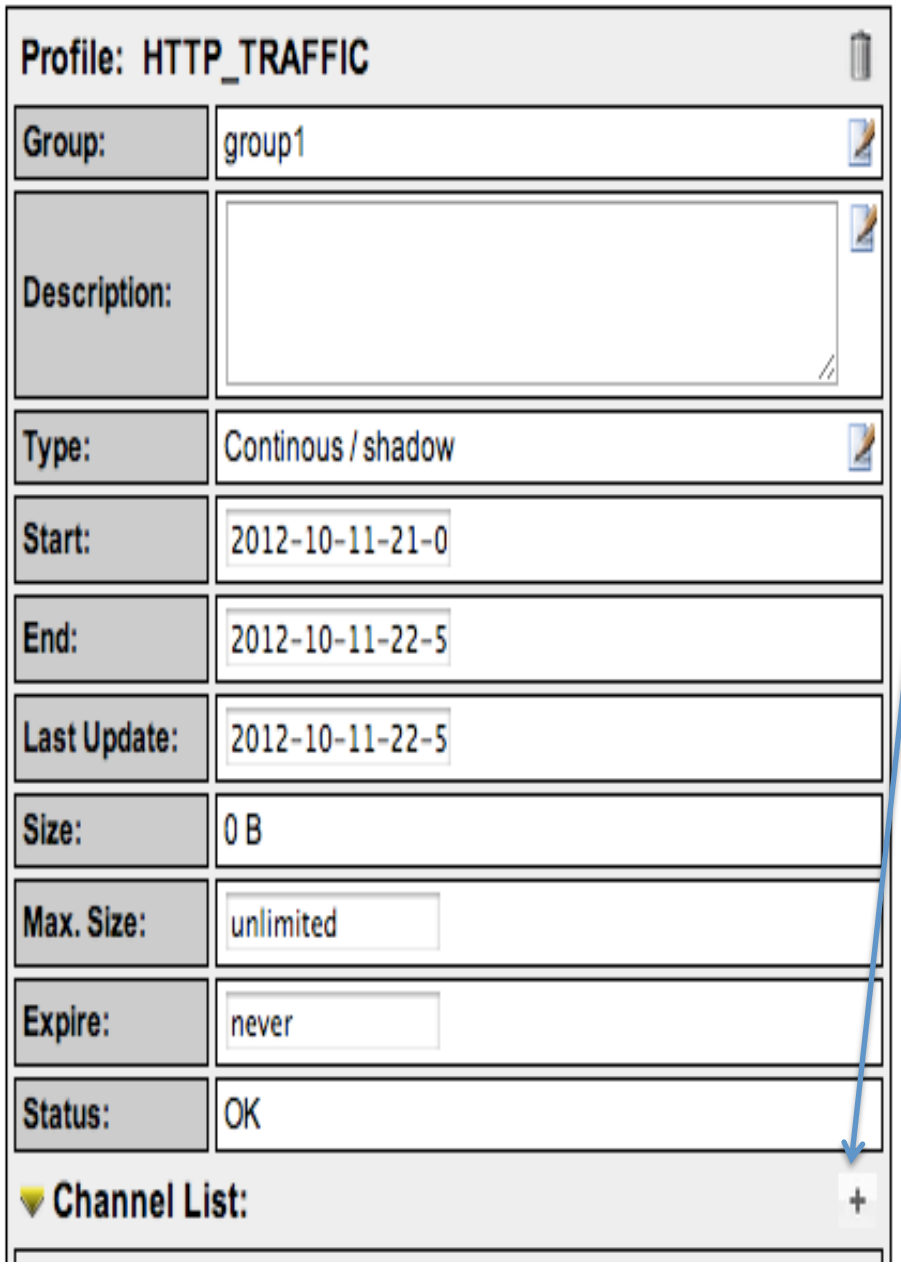
Création d'un graphe pour un traffic particulier

- Sur le PC qui reçoit les flux, ouvrir la page NfSEN et cliquer sur 'live' en haut à droite de la page, et selectionner "New Profile*".*
  - *NfSen peut être réticent: réssayer!*
- Taper le nom 'HTTP_TRAFFIC' pour le nom du profile et créer un nouveau groupe appelé "groupeX" ou X est le numéro de votre groupe.
- Choisir un canal (channel) et des profiles "shadow".
  - Canal individuel– créer un canal avec nos propres filtres
  - Profil "shadow"– on économise de l'espace disque en ne créant pas de nouvelles données, on analyse l'existant

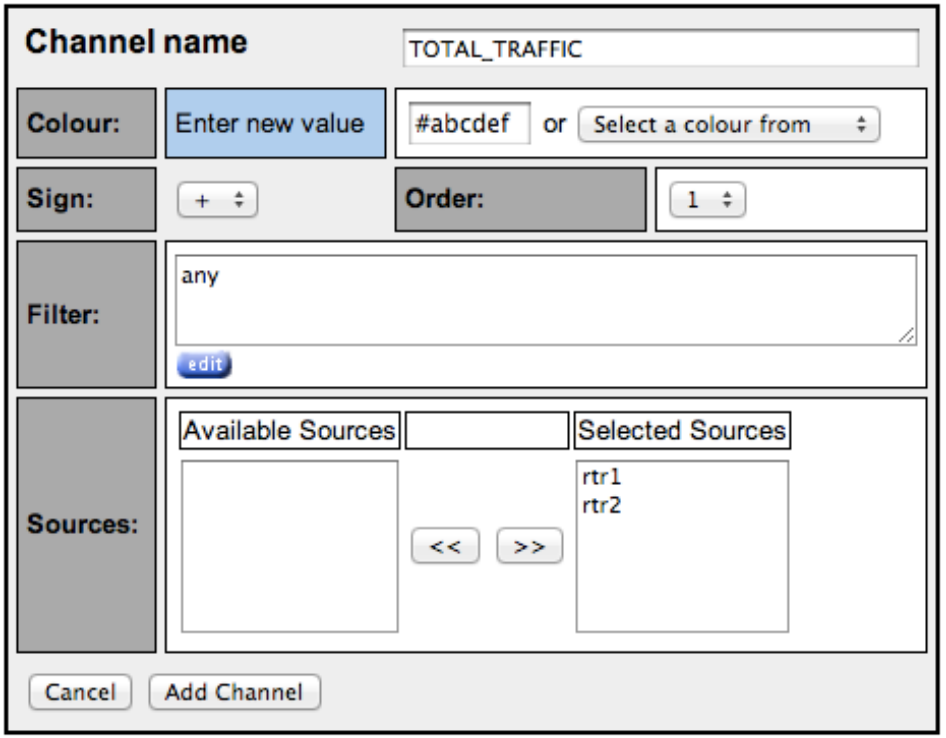
➔ **Voir la page suivante pour une illustration…**

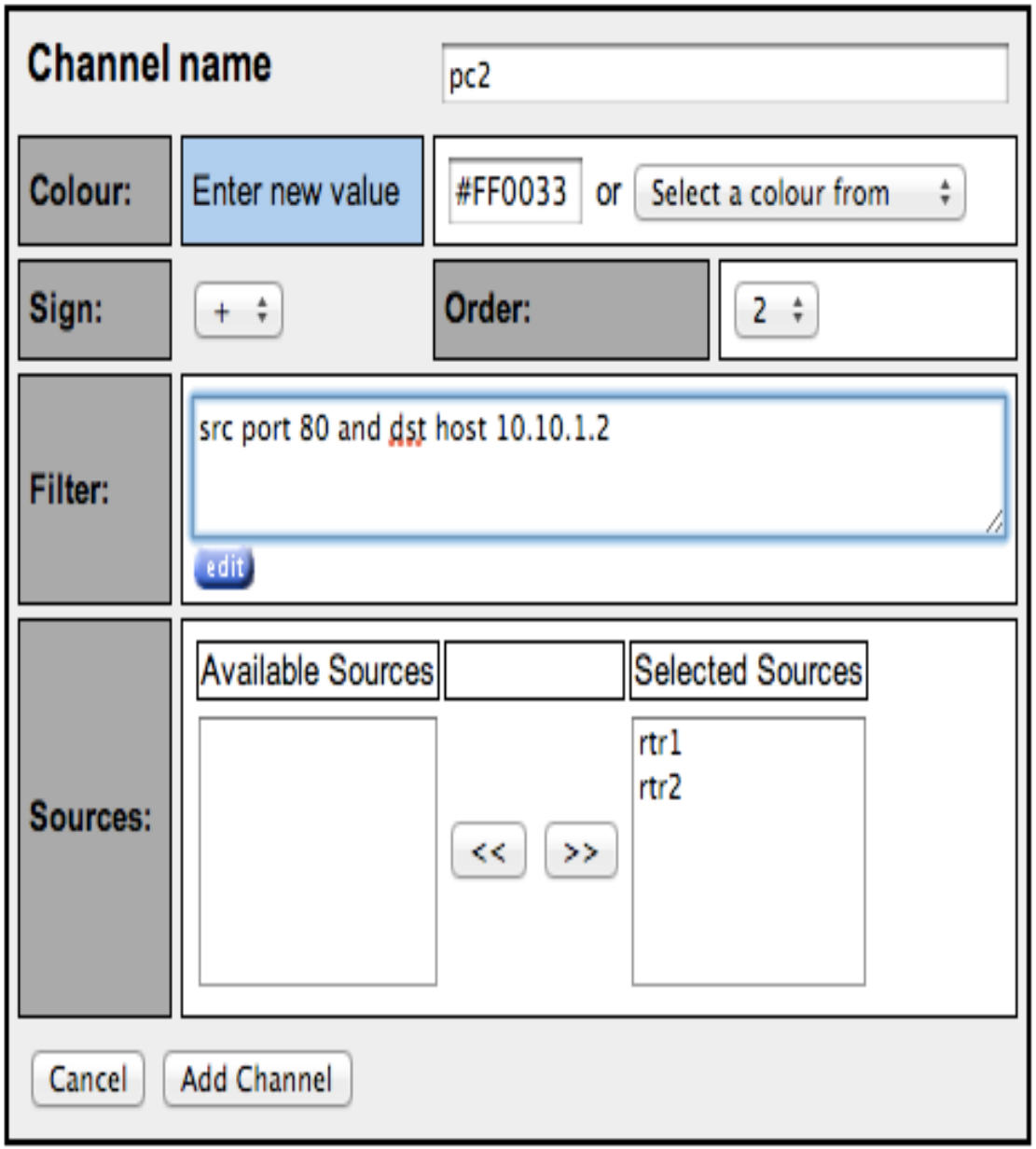


Cliquer “Create Profile” en bas du menu.



Cliquer sur le sign (+) à côté de la 'Channel List' en bas de page, puis rempir la page suivante comme ci-dessous, et cliquer sur 'Add Channel' en bas.
Le filtre "any" signifie TOUT le traffic.
Choisir les sources dans "Available Sources" et cliquer sur ">>" pour les ajouter aux "Selected Sources" (choisies), puis "Add Channel"





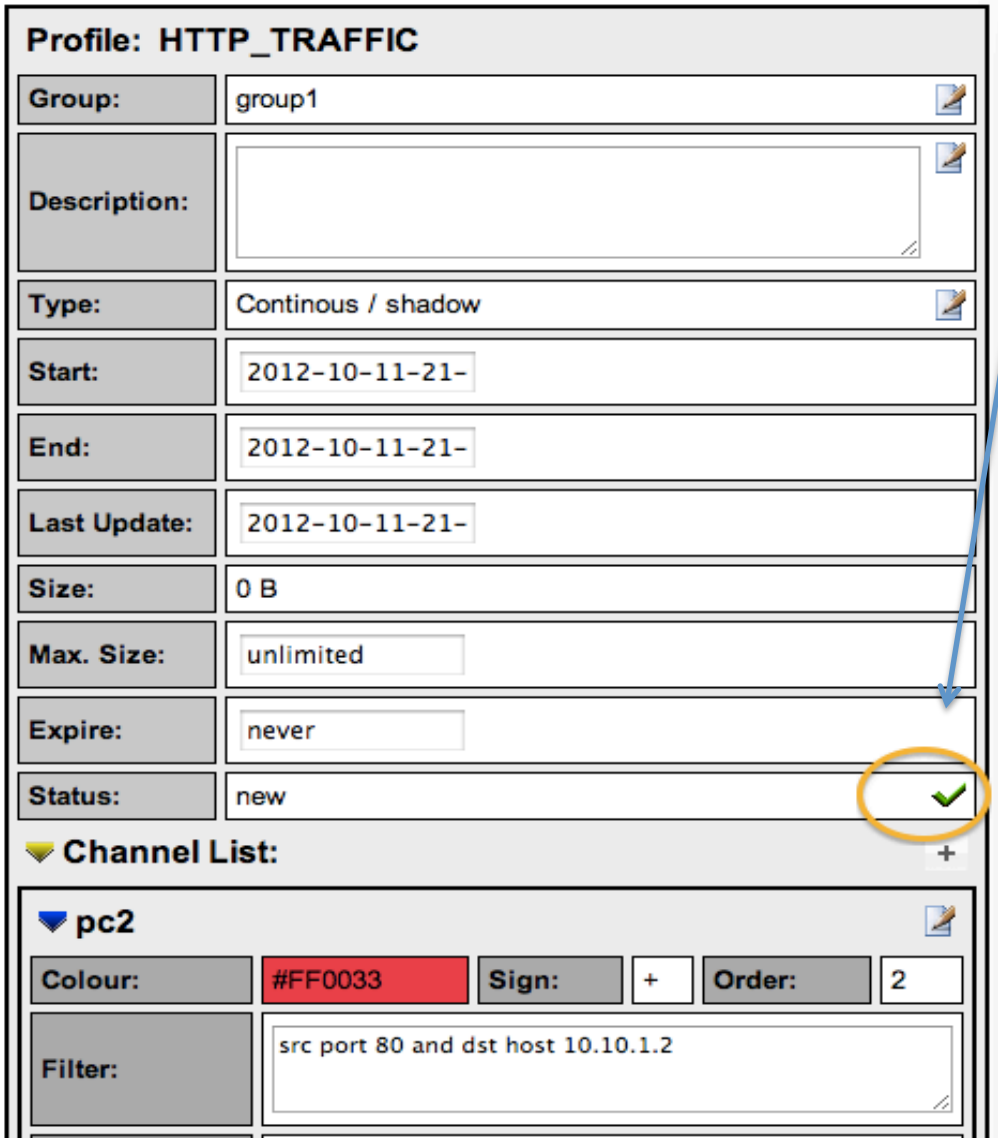
Ajouter un autre canal (channel) en cliquant sur le signe (+) comme avant, à côté de 'Channel List'. Remplir les détails comme indiqué à gauche. Remplacer pc2 avec le numéro d'un PC qui ne soit pas le vôtre! Remplacez également l'adresse IP dans le Filtre pour qu'elle corresponde à l'IP du PC en question.

Avec ceci, nous traquerons combien de traffic HTTP va vers ce PC. C'est à dire, la quantité télechargée. En HTTP, le port source est toujours le port 80.

Ne pas oublier de changer la couleur. Vous pouvez utiliser la lliste des couleurs ou entrer votre propre valeur.

Choisir les deux routeurs comme source, et cliquer sur 'add channel'

Activation du profil



- Cliquer sur la coche verte pour activer le nouveau profil.
- Cliquer sur Live et choisir “HTTP_TRAFFIC” et vous verrez votre profil. Puis cliquer sur la “Home” dans le menu en gaut à cauche de la page NfSen.

Récupérer des données en HTTP sur PCy

Logez vous sur le PCy (défini précédemment dans le canal) et utiliser la commande `wget` pour simuler un téléchargement sur pcY.

```
ssh sysadm@pcY.ws.nsrc.org
$ cd /tmp
$ wget http://noc.ws.nsrc.org/downloads/BigFile
```

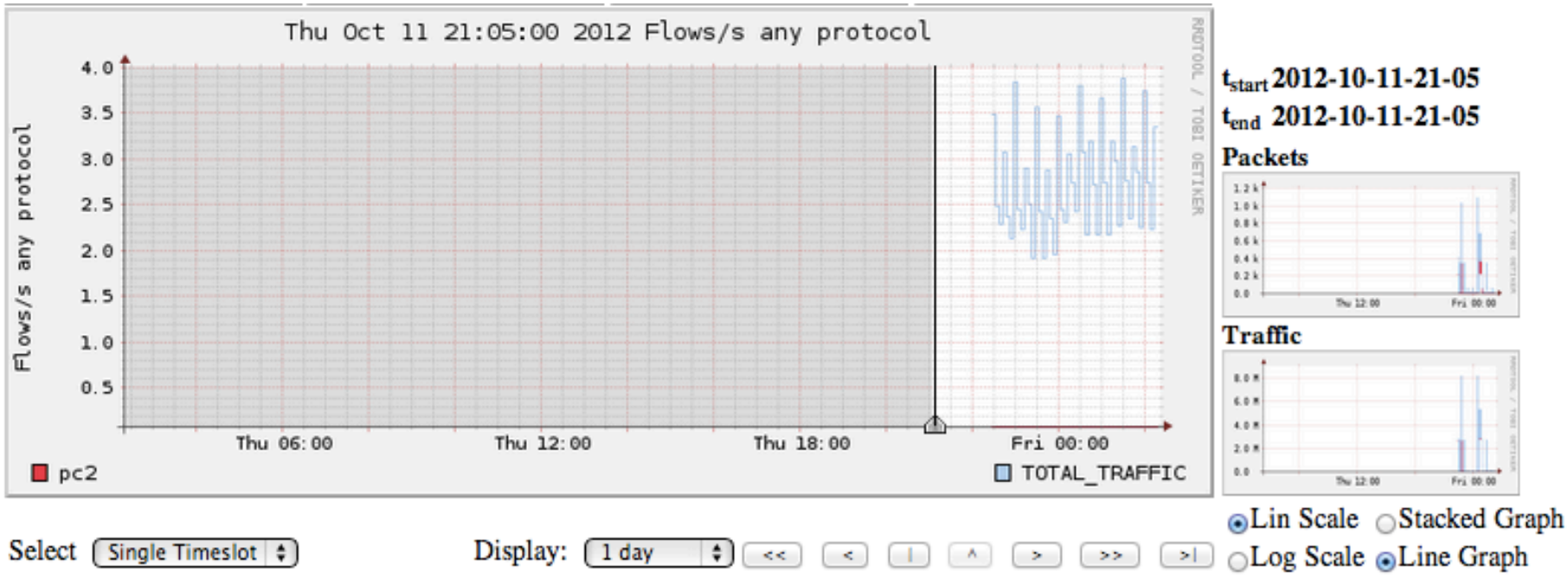
Une fois le téléchargement fini, vous pouvez effacer le fichier:

```
$ rm /tmp/BigFile
$ exit                    (pour vous déconnecter)
```

Voir le traffic

Ceci peut prendre jusqu'à 15 minutes avant que ce soit à jour.

Aller à 'Graphs' puis 'Traffic'. Puis Details, et choisir 'Line Graph' en bas.

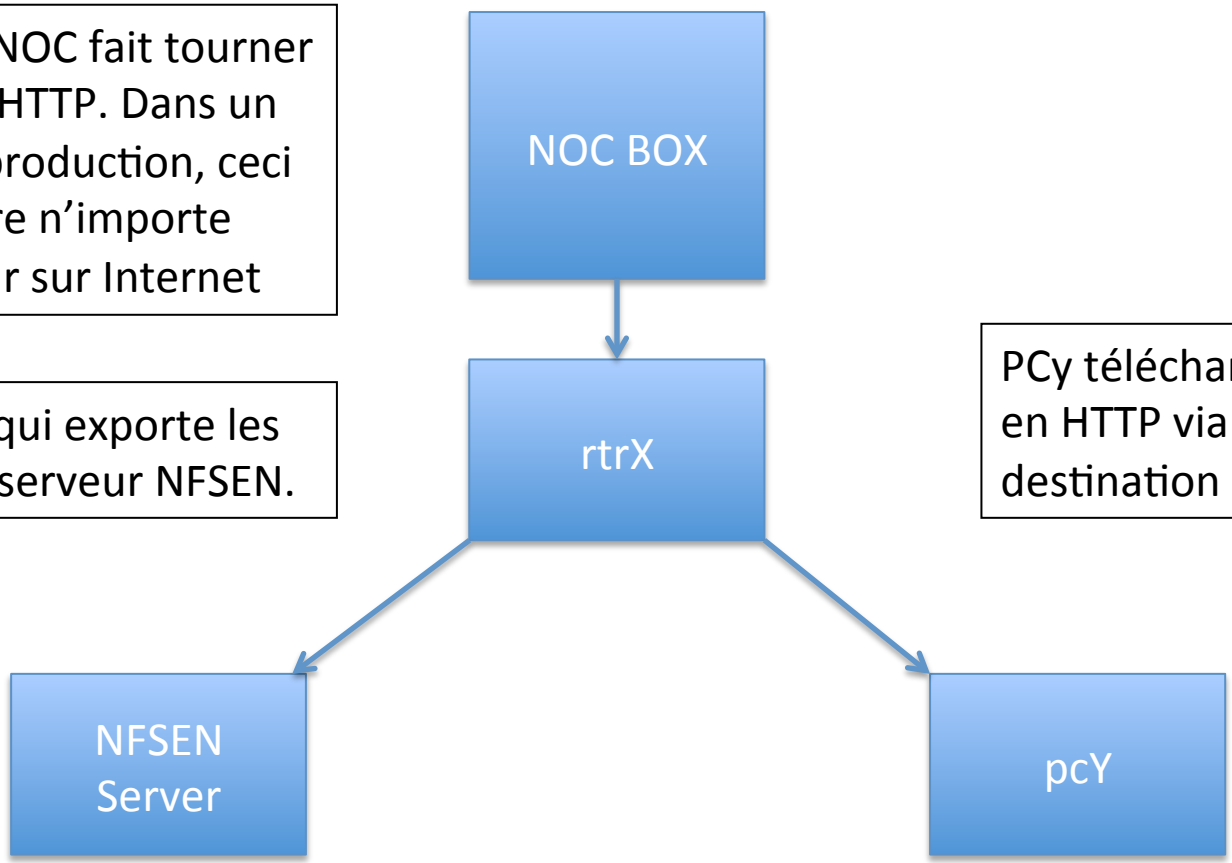


C'est un graphe du traffic total qui traverse votre routeur rtrX **et le traffic HTTP du téléchargement depuis pcY**

Moment de réflexion

Le serveur NOC fait tourner un serveur HTTP. Dans un réseau de production, ceci pourrait être n'importe quel serveur sur Internet

Le routeur qui exporte les flux vers le serveur NFSEN.



PCy télécharge un fichier en HTTP via rtrX et est la destination (dst host)

On a indiqué à NFSEN de grapher le traffic dont le port source est 80 et la destination est 10.10.X.Y. Vous pouvez faire la même chose sur votre réseau de production, en ajoutant un graphe pour des serveurs web précis, par exemple "src host a.b.c.d" ou a.b.c.d sons les adresses IP des serveur web de FaceBook par exemple.

Observer un téléchargement FTP depuis le NOC

- Même travail (transparents 5 et suivants) from mais cette fois-ci, mettre ‘FTP_TRAFFIC’ à la place de ‘HTTP_TRAFFIC’
- FTP n’utilise pas toujours le port 20 pour les données. On sait que ça sera un port supérieur à 1024, donc le filtre doit contenir:
  `src port > 1024 and dst host 10.10.X.Y`
- Choisir la bonne source depuis Available Sources
- Maintenant, nous allons récupérer un gros fichier par FTP depuis le NOC vers pcY.ws.nsrc.org
- ➔ **Instructions sur la page suivate…**

Récupérer les données en FTP depuis le NOC

Loggez vous sur le pcY et utilisez la commande `ftp` pour récupérer le fichier depuis le NOC

```
ssh sysadm@pcY.ws.nsrc.org

$ ftp noc.ws.nsrc.org
   Name (noc.ws.nsrc.org:sysadm): anonymous
   Password:   <YourEmailAddress>
   ftp> lcd /tmp
   ftp> get BigFile          (il faut attendre…)
   ftp> quit

$ rm /tmp/BigFile
```

Le graphique prendra jusqu'à 15 minutes pour être mis à jour. Aller à Graphes, puis Traffic. Ensuite regarder Details et choisir 'Line Graph' en bas pour voir le résultat.

Part 2

Grapher une interface particulière sur le routeur

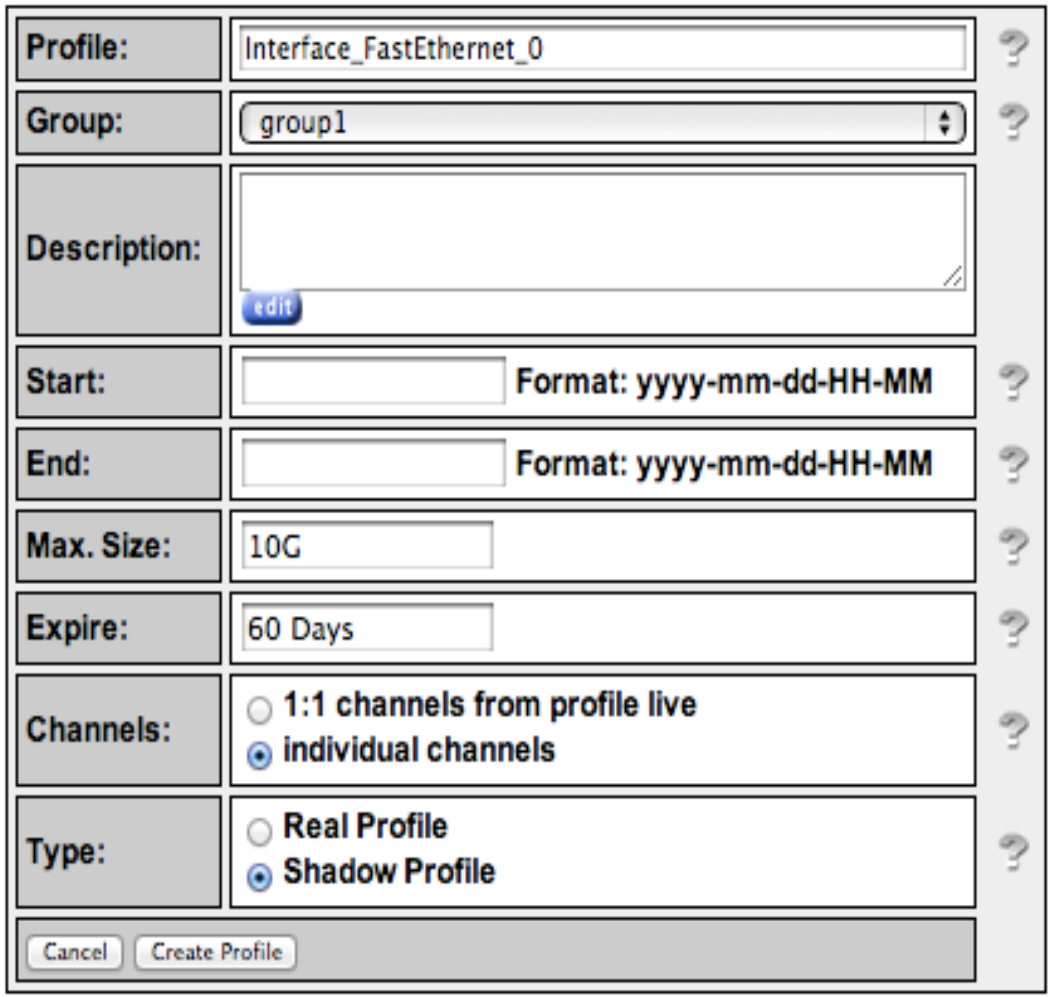
- Utiliser la commande *snmpwalk* de votre PC pour déterminer l'indice "ifIndex" de l'interface que vous voulez grapher:

```
$ snmpwalk -v2c -c NetManage rtrX.ws.nsrc.org ifDescr

IF-MIB::ifDescr.1 = STRING: FastEthernet0/0
IF-MIB::ifDescr.2 = STRING: FastEthernet0/1
IF-MIB::ifDescr.3 = STRING: VoIP-Null0
IF-MIB::ifDescr.4 = STRING: Null0
IF-MIB::ifDescr.5 = STRING: Loopback0
```

- Cela veut dire que l'interface F0/0 a l'indice numéro 1. Nous pouvons utiliser NfSen pour voir le traffic sur cette interface particulière
  - NetFlow doit être activé sur cette interface
  - Grâce à "snmp ifindex persist", l'indice de l'interface ne change pas

Ajouter l'interface à NfSen

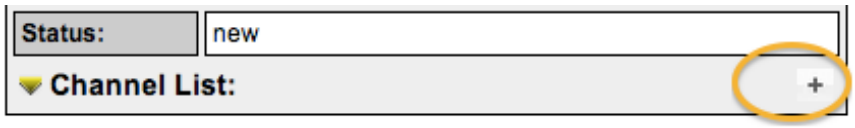


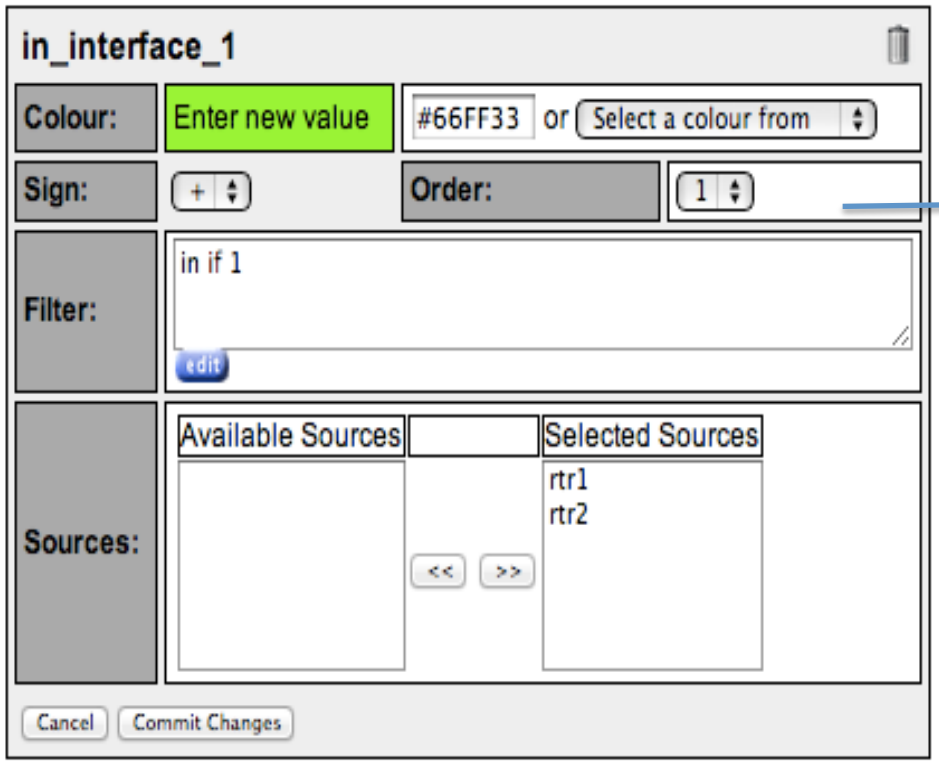
Cliquer sur Live et choisir "New Profile…"

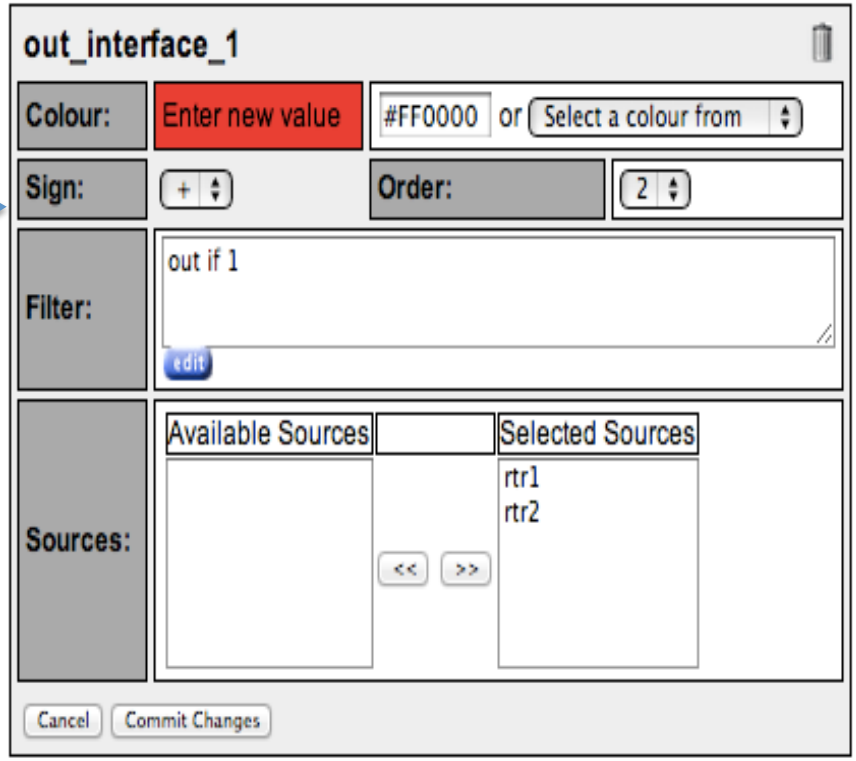
Donner au Profile un nom adéquat et ajoutez le au groupe que vous créé préalablement

Choisir des canaux individuels et des Shadow profile comment avant, et cliquez sur "Create Profile"

Sur l'écrant suivant, cliquer sur le signe "+" à côté de la liste des canaux







Ceci signifie que tout le trafic ENTRANT sur l'interface 1 sera graphée. Cliquer sur "Add Channel" et cliquer + pour ajouter un deuxième canal.

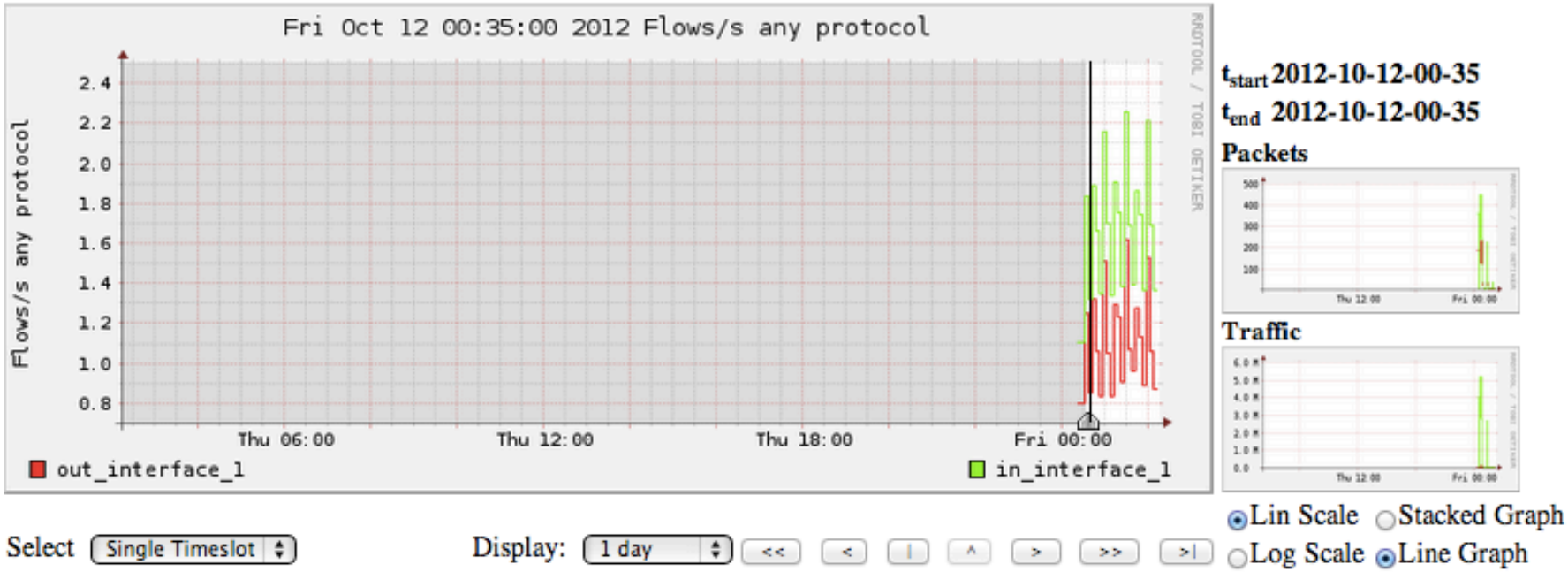
NOTE: L'interface "1" fait référence au numéro d'indice de l'interface "FastEthernet 0/0" sur rtrX

Ceci signifie que tout le trafic SORTANT sur l'interface 1 sera graphé. Cliquer sur "Add Channel" puis activer le filtre sur l'écrant suivant en cliquand sur la coche verte.

Être patient pour que les données ait le temps d'être collectées. Comparer avec le graphe de Cacti…

Voir le traffic

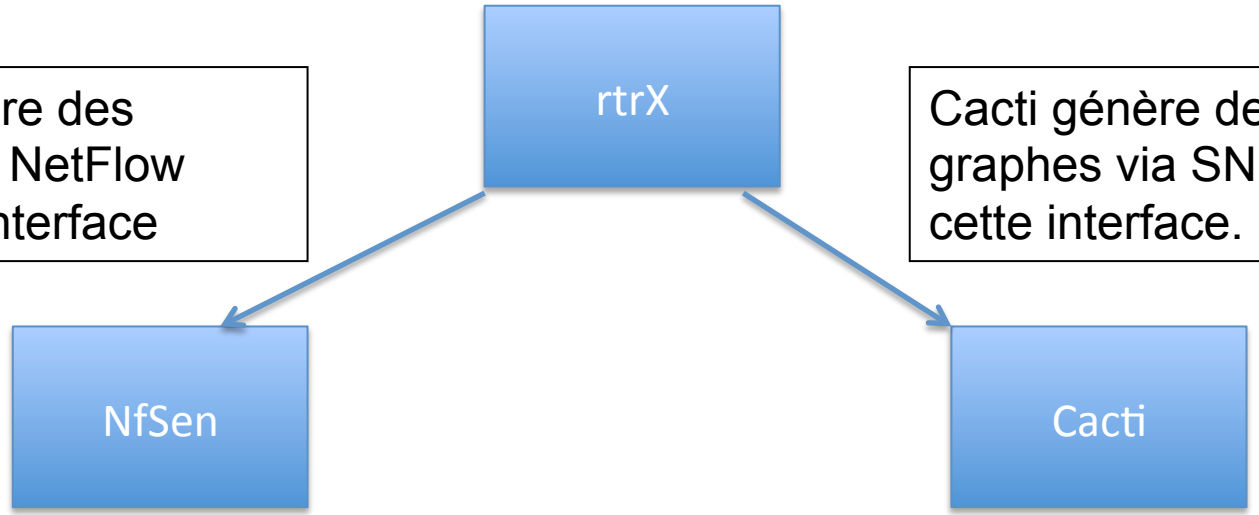
Il faudra jusqu'à 15 minutes pour que ce graphe soit mis à jour. Aller à Graphs puis Traffic. Puis choisir 'Line Graph' dans les options en bas à droite.



Ceci est un graphe du trafic total passant au travers du routeur rtrX sur l'interface FastEthernet 0/0.

Stop! Moment de réflexion

NfSen génère des graphes via NetFlow pour cette interface



Cacti génère des graphes via SNMP pour cette interface.

Avec NfSen, on peut utiliser les fonctionnalitées de NetFlow pour extraire plus d'informations, comme par exemple quelles adresses IP sont actives, quels sont les ports élevés qui utilisent le plus d'octets, et quels sont les numéros d'AS qui entrent/sortent de notre réseau – et bien plus!

Stop! Moment de réflexion

NfSen génère des graphes via NetFlow pour cette interface

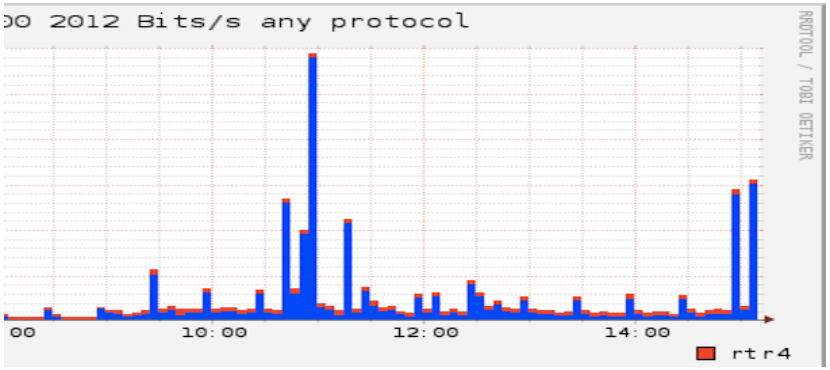
rtrX

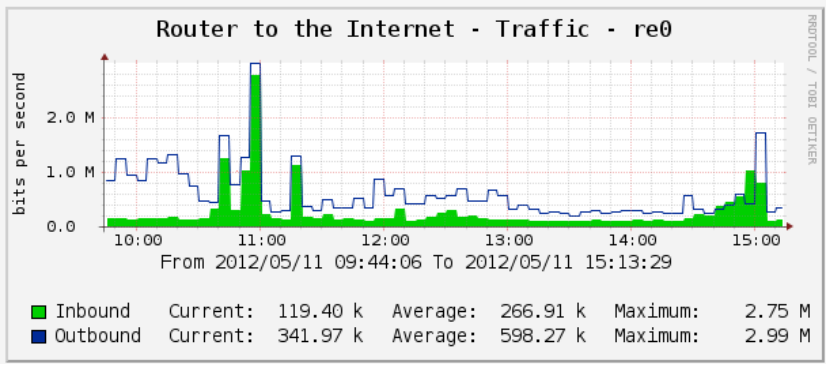
Cacti génère des graphes via SNMP pour cette interface.

NfSen

Cacti

Si vous mesurez la même interface avec Cacti et NfSen, alors vous devriez pouvoir obtenir des graphes similaires, pour ce qui est des Bit / s.





Part 3

NetFlow avancé

Aller sur Profile, sélectionner un groupe que vous avez créé puis choisir ‘HTTP_TRAFFIC’. Cliquer sur l’onglet ‘Detail’, choisir ‘Time Window’ plutôt que ‘Time Slot’, sous le graphe. Choisir une partie du graphe qui montre de l’activité (des pics) comme ci-dessus.

Options:

○ List Flows ◉ Stat TopN

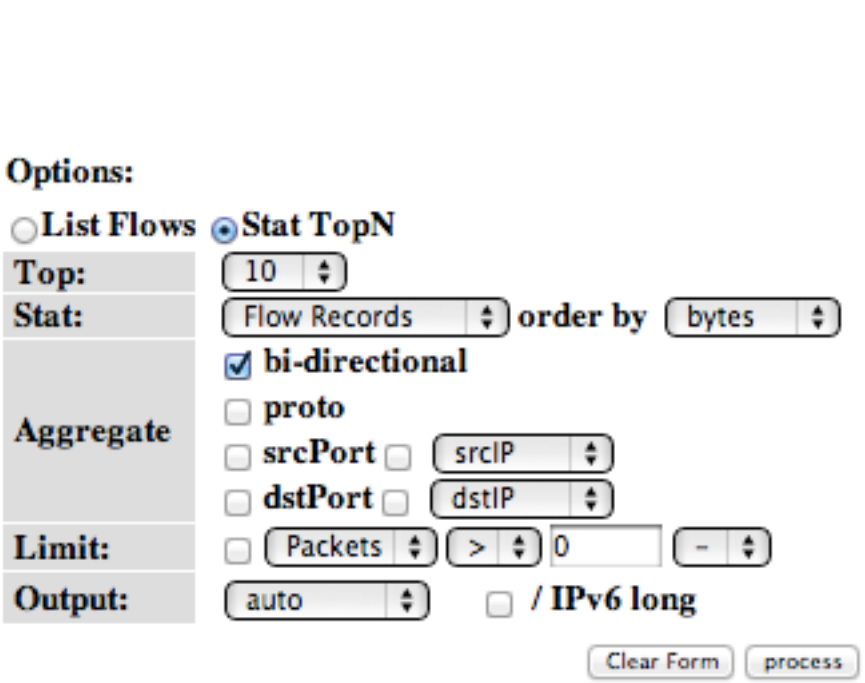
Top:	10
Stat:	Flow Records **order by** bytes
Aggregate	☐ **bi-directional** ☑ **proto** ☑ **srcPort** ☑ srcIP ☑ **dstPort** ☑ dstIP
Limit:	☐ Packets > 0 -
Output:	auto ☐ **/ IPv6 long**

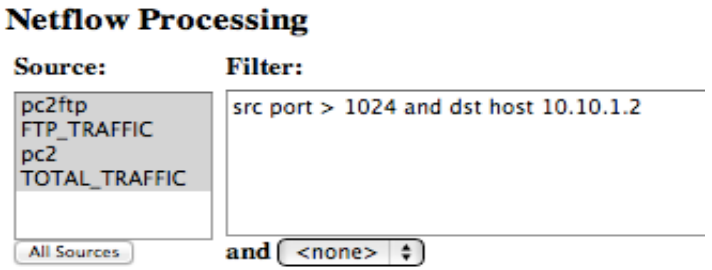
Clear Form process

Choisir les options comme à gauche. Ceci veut dir, choisir le Top 10 des Flux, Trier par octet du plus gros au plus bas, et afficher les informations pour les adresses et port source et destination. Puis cliquer sur 'Process'. Analyser la sortie que vous obtiendrez et qui ressemblera à l'exemple ci-dessous.

Aggregated flows 53723
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
2012-05-09 16:31:43.481	664.018	TCP	10.10.0.60	53731	10.10.0.250	22	1.0 M	1.5 G	18.1 M	1482	1
2012-05-09 17:10:21.896	722.117	TCP	10.10.0.254	42499	10.10.8.29	22	310886	466.2 M	5.2 M	1499	47
2012-05-09 16:22:44.095	4108.913	TCP	208.117.226.27	80	10.10.0.77	49757	69250	103.7 M	201865	1497	2
2012-05-09 18:13:16.475	45.837	TCP	10.10.0.60	54946	10.10.0.250	22	66924	99.5 M	17.4 M	1487	1
2012-05-09 18:18:45.625	39.212	TCP	10.10.0.250	16647	10.10.0.60	54987	66230	99.3 M	20.3 M	1499	1





Essayez la même chose avec l'option Bi-directional. Que voyez-vous ? Essayer les différentes options pour voir quels résultats vous obtiendrez. Vous pouvez aussi ajouter ces même filtres dans le fenêtre de filtre, à côté des Options.

Essayer les filtres suivants:

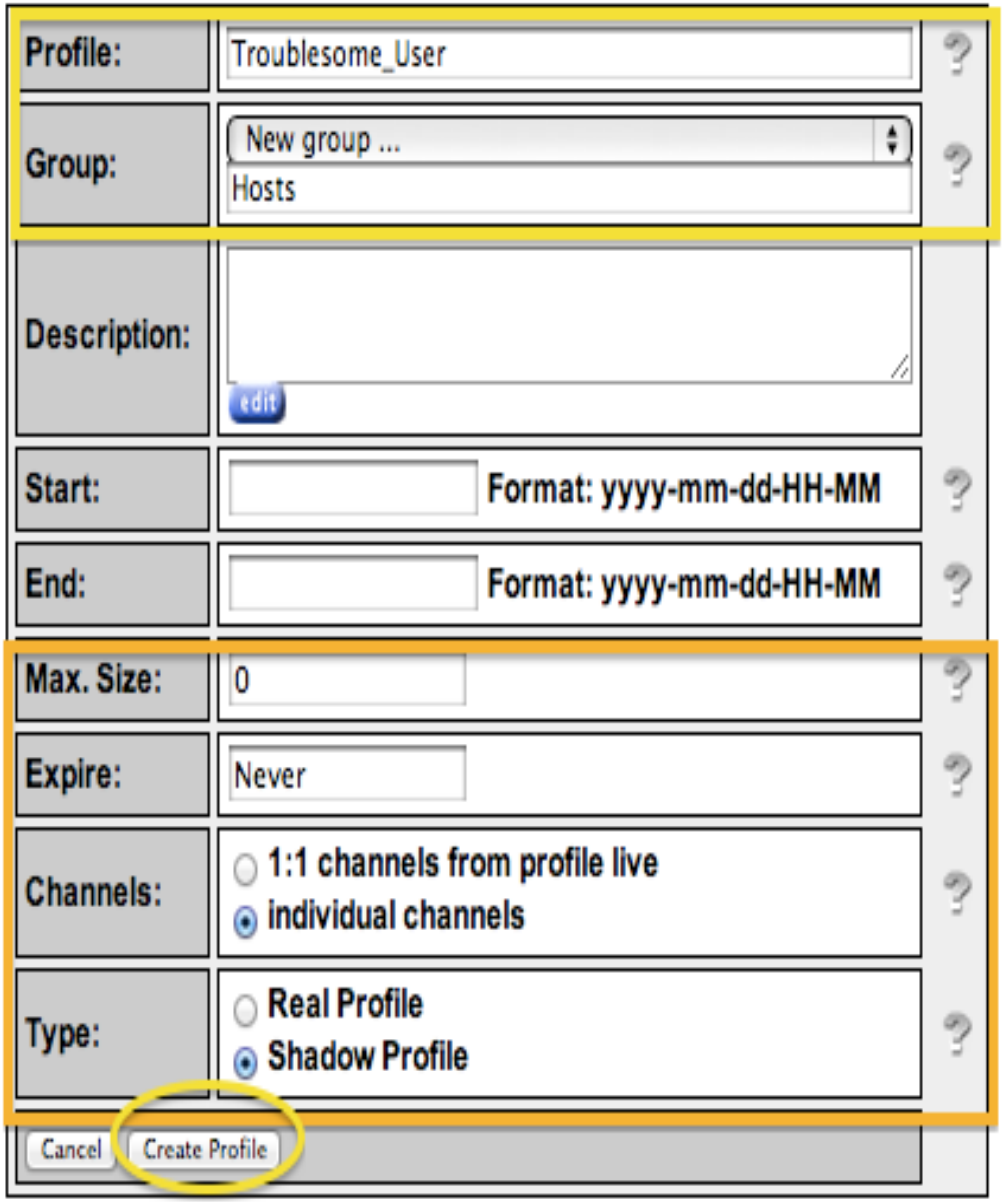
src host 10.10.X.Y – chercher le trafic provenant de cette machine
src port 22 – les flux ou le port source est 22
src port 22 or src port 80 – les flux de port source 22 ou 80
src port 80 and in if 1 – les flux de port source 80 et sur l'interface 1
dst net 10.10.0.0/16 – tous les flux dont le réseau de destination est is 10.10.0.0/16
src port > 5000 – tous les flux don't le port source est supérieur à 5000

Beaucoup de filtres disponibles

- Si vous vouliez voir par numéro d'AS, pour Google:
  - `src as 15169`
- Vous pouvez faire ceci pour n'impore quelle AS mais votre routeur doit avoir une copie de la table de routage installée, et '*ip flow-export version 9 origin-as'* configuré.
- On peut alors faire des graphes pour chacun d'entre eux comme précédemment
- Les filtres en détail: http://nfsen.sourceforge.net/#mozTocId652064

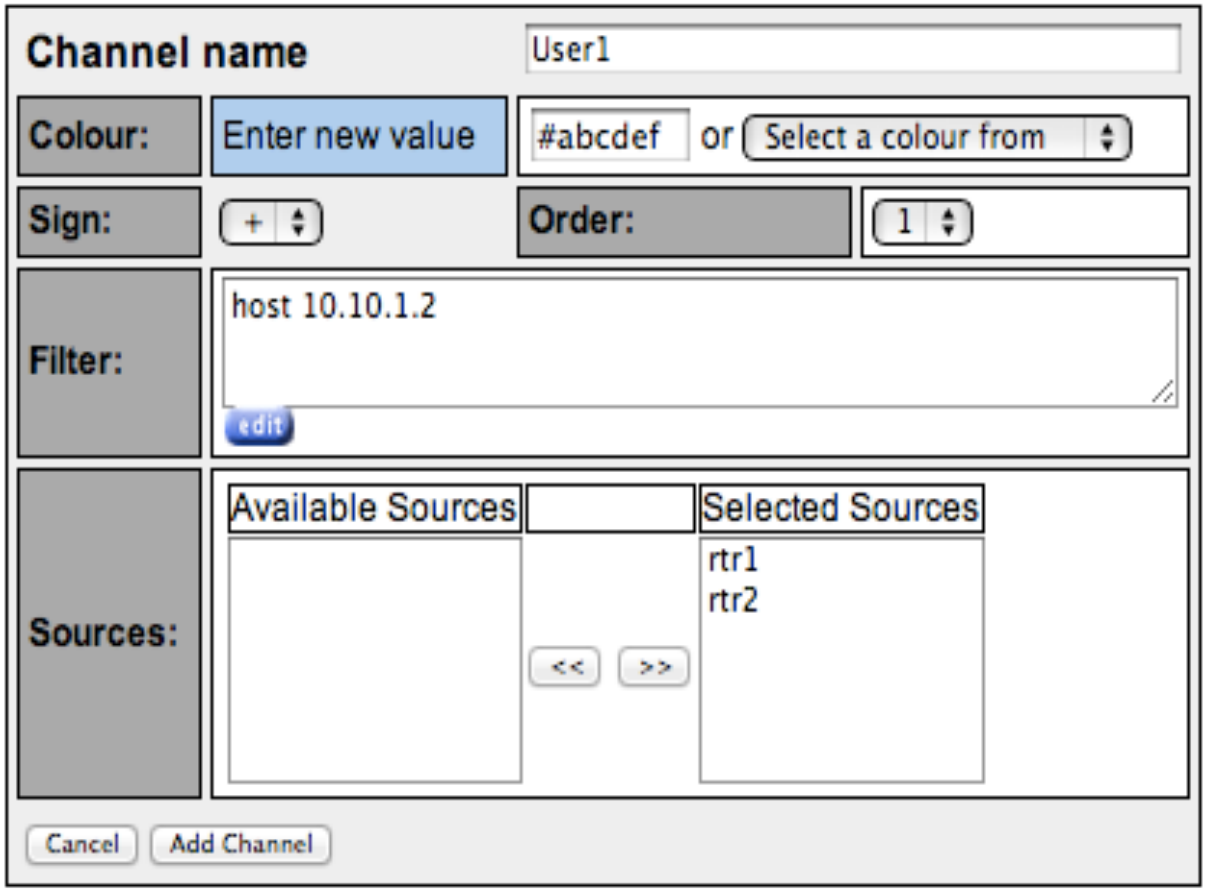
FACULTATIF

Surveiller une machine particulière



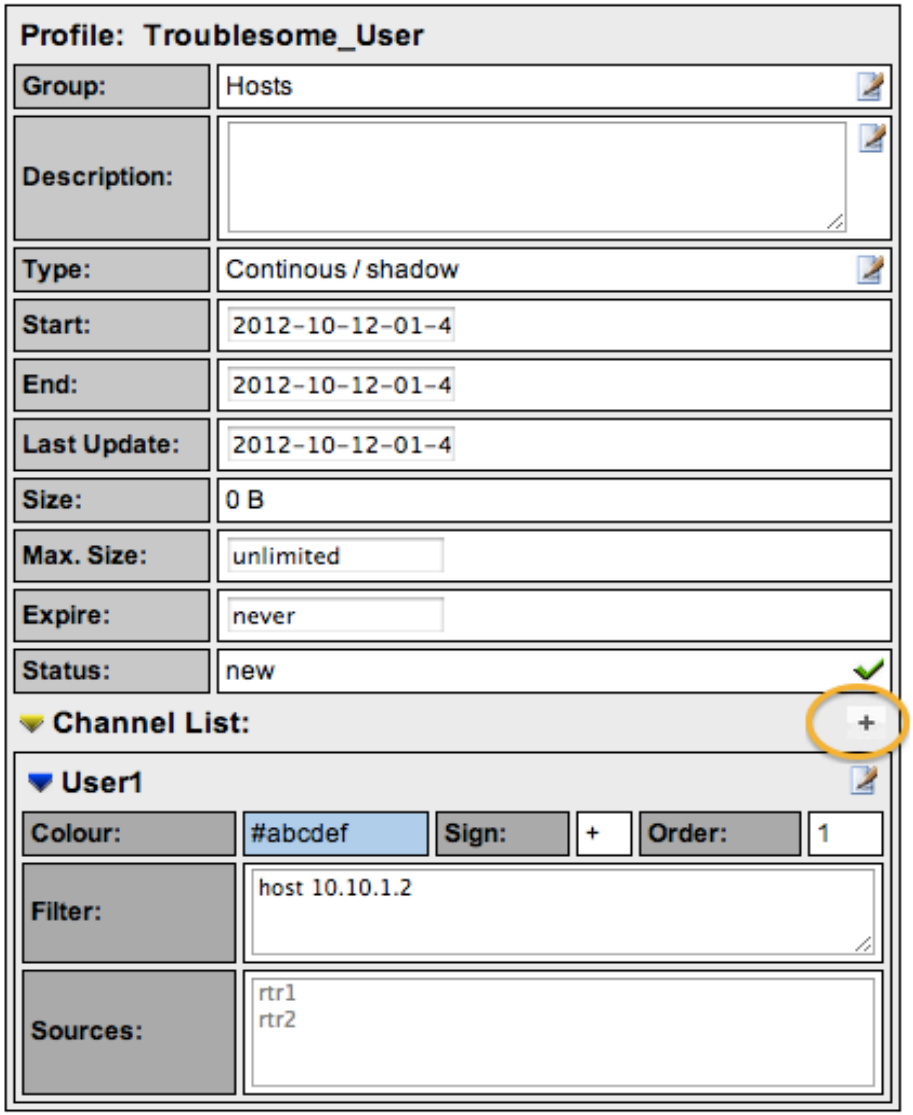
- Sur le menu “Profile” de NfSen, choisir “New Profile…”
- Ensuite cliquer sur “Create Profile” en bas
- Vous verrez un message “new profile created”
- Cliquer sur le signe “+” en bas pour créér des canaux.

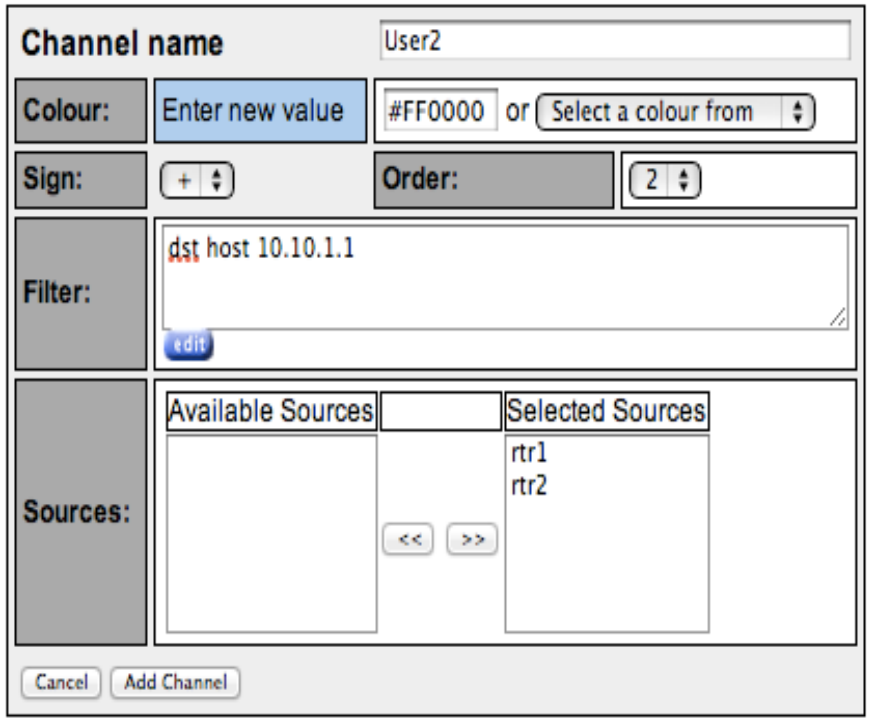
Monitor a Specific IP



Remplacer 10.10.1.2 avec l'IP de votre machine virtuelle.

Ajouter un second canal



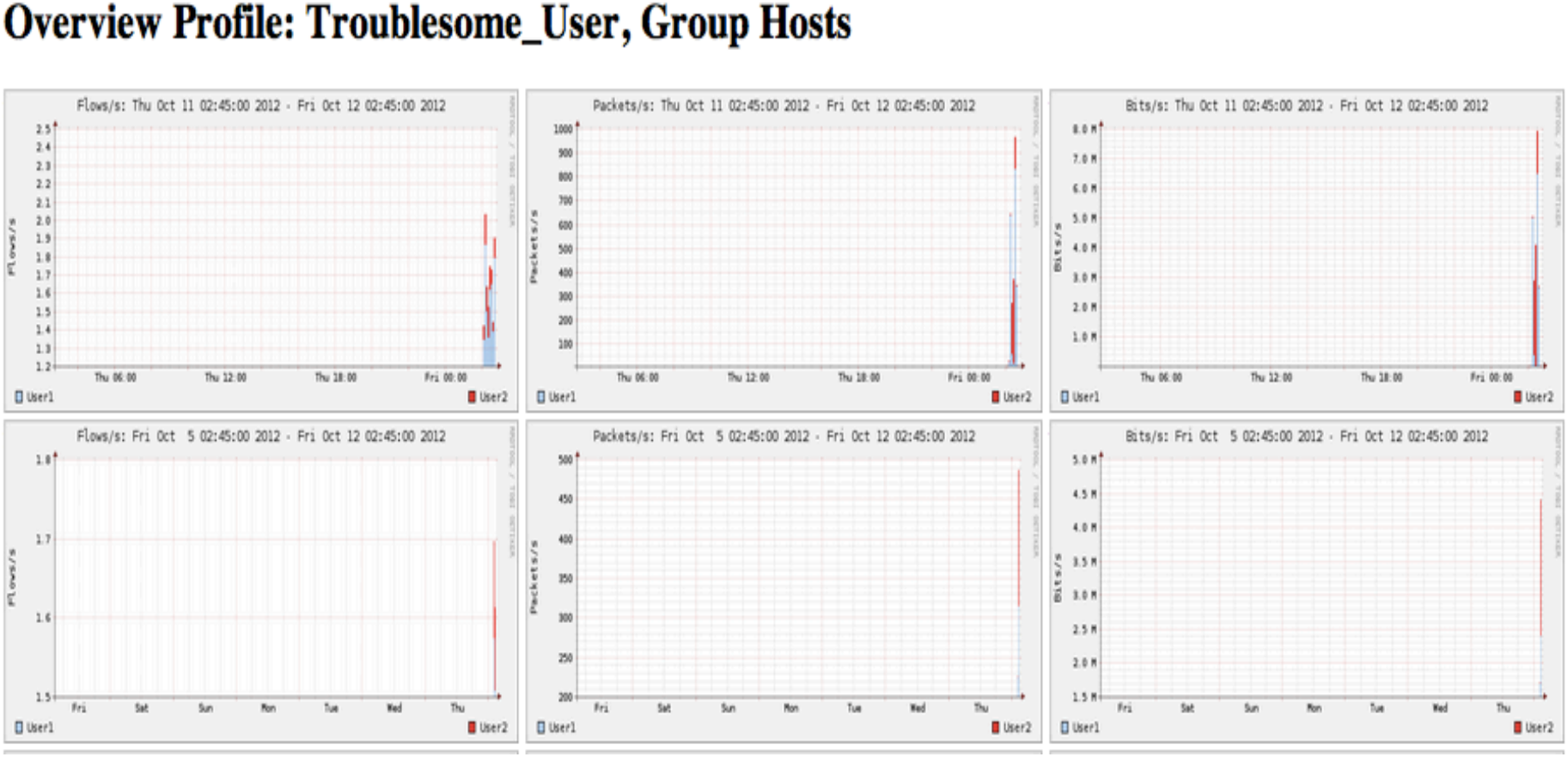


Cliquer sur “Add Channel” puis cliquer sur la coche verte pour activer le nouveau profile “Troublesome_User” (utilisateur pénible)

Filters

- Choisir une couleur différente pour le deuxième canal pour que les graphes puissent se distinguer
- Noter que les deux filtres sont différents
  - Le premier filtre ne capture que les flux provenant d'un du premier pc
  - Le second filtre ne capture que les flux où la destination est la deuxième machine
  - Pour générer du trafic visible sur le graphe, essayez de transférer des fichier depuis la première machine, vers la seconde.
- D'autres paramètres peuvent être ajoutés comme l'AS source, l'AS destination, ports sources et dst, etc., basée sur la syntaxe des filtres NfSen

Évolution des tendances



PASSER À L’EXERCICE 5

Plugin PortTracker