



NFSEN Exercise - 3

What we will do

- 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 le type de trafic traverse ces deux routeurs

Création d'un graphe pour un trafic particulier

- Sur le PC qui reçoit les flux, ouvrir la page NfSEN et cliquer sur 'live' en haut à droite de la page, et sélectionner "New Profile".
 - Taper le nom 'HTTP_TRAFFIC' pour le nom du profile et créer un nouveau groupe appelé "groupX" 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...**

Profile:	<input type="text" value="HTTP_TRAFFIC"/>	?
Group:	<input type="text" value="New group ..."/> <input type="text" value="group1"/>	?
Description:	<div style="border: 1px solid gray; height: 60px; width: 100%;"></div> <input type="button" value="edit"/>	
Start:	<input type="text"/> Format: yyyy-mm-dd-HH-MM	?
End:	<input type="text"/> Format: yyyy-mm-dd-HH-MM	?
Max. Size:	<input type="text" value="10G"/>	?
Expire:	<input type="text" value="60 Days"/>	?
Channels:	<input type="radio"/> 1:1 channels from profile live <input checked="" type="radio"/> individual channels	?
Type:	<input type="radio"/> Real Profile <input checked="" type="radio"/> Shadow Profile	?
<input type="button" value="Cancel"/> <input type="button" value="Create Profile"/>		

Cliquer "Create Profile" en bas du menu.

Profile: HTTP_TRAFFIC	
Group:	group1
Description:	
Type:	Continuous / shadow
Start:	2012-10-11-21-0
End:	2012-10-11-22-5
Last Update:	2012-10-11-22-5
Size:	0 B
Max. Size:	unlimited
Expire:	never
Status:	OK
Channel List:	

Cliquer sur le sign (+) à côté de la 'Channel List' en bas de page, puis remplir la page suivante comme ci-dessous, et cliquer sur 'Add Channel' en bas.

Le filtre "any" signifie TOUT le trafic. Choisir les sources dans "Available Sources" et cliquer sur ">>" pour les ajouter aux "Selected Sources" (choisies)

Channel name	TOTAL_TRAFFIC	
Colour:	Enter new value	#abcdef or Select a colour from ▾
Sign:	+ ▾	Order: 1 ▾
Filter:	any <small>edit</small>	
Sources:	Available Sources	Selected Sources
		rtr1 rtr2
	<< >>	
<input type="button" value="Cancel"/> <input type="button" value="Add Channel"/>		

Channel name

Colour: or

Sign: **Order:**

Filter:

Sources:

Available Sources	Selected Sources
	rtr1 rtr2


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 reçoit **PAS de flux** dans votre groupe. 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 trafic HTTP va vers ce PC. C'est à dire, la quantité téléchargée. En HTTP, le port source est toujours le port 80.

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

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

Activation du profil

Profile: HTTP_TRAFFIC	
Group:	group1
Description:	
Type:	Continuous / shadow
Start:	2012-10-11-21-
End:	2012-10-11-21-
Last Update:	2012-10-11-21-
Size:	0 B
Max. Size:	unlimited
Expire:	never
Status:	new 
▼ Channel List: +	
▼ pc2	
Colour:	#FF0033
Sign:	+
Order:	2
Filter:	src port 80 and dst host 10.10.1.2

- 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 haut à gauche 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
```

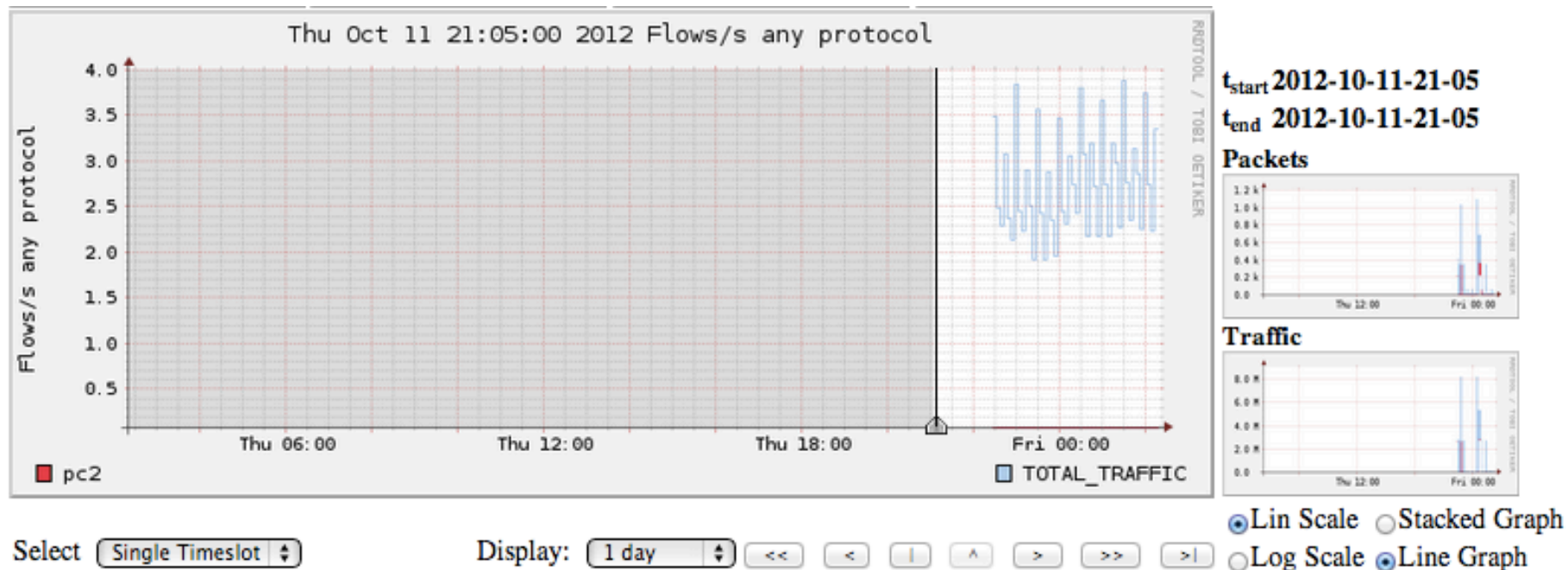
Une fois le téléchargement fini, vous pouvez effacer le fichier:

```
$ rm /tmp/BigFile
$ exit
```

(pour vous déconnecter)

Voir le trafic

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 trafic total qui traverse votre routeur
rtrX et le trafic 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.

NOC BOX

rtrX

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

NFSEN
Server

pcY

On a indiqué à NFSEN de grapher le trafic 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 sous les adresses IP des serveur web de FaceBook par exemple.

Observer un téléchargement FTP depuis le NOC

- Même travail (transparentes 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 suivante...**

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.