% Supervision NetFlow
%
% Gestion et Surveillance de Réseau

Introduction

Objectifs

* Apprendre à installer les outils nfdump et NfSen

Notes

* Les commandes précédées de "$" signifient que vous devez exécuter
  la commande en tant qu'utilisateur général - et non en tant
  qu'utilisateur root.
* Les commandes précédées de "#" signifient que vous devez
travailler
  en tant qu'utilisateur root.
* Les commandes comportant des lignes de commande plus spécifiques
  (par exemple "RTR-GW>" ou "mysql>") signifient que vous exécutez
  des commandes sur des équipements à distance, ou dans un autre
  programme.

Prérequis

Il est attendu que vous ayez déja configuré votre routeur pour
exporter
les flux vers un PC dans votre groupe et que votre groupe voisin a
configuré
leur routeur pour qu'il exporte les flux vers le même PC. Voir
l'exercice 1
pour les détails.

Configurer votre collecteur

Installer Nfdump et les outils associés.

Nfdump fait partie des outils de collection Netflow. Nous allons
installer plusieurs outils supplémentaires dont nous aurons besoin
un peu plus tard.

~~~~~~
~~~~~~~
$ sudo apt-get install rrdtool mrtg librrds-perl librrdp-perl
librrd-dev \
libmailtools-perl php5 bison flex
~~~~~~
~~~~~~

~~~~~~~

Si on vous demande "Make /etc/mrtg.cfg owned by and readable only by
root?"
choisir "<Yes>" et appuyer sur ENTREE pour continuer.

Compilation et installation de nfdump

Il nous manque des outils:

nfcapd, nfdump, nfreplay, nfexpire, nftest, nfgen

Il y a un paquetage dans Ubuntu mais celui ci est trop ancien.
Nous avons donc re-compilé un paquetage plus récent, prêt à être
téléchargé du NOC:

~~~~~~
~~~~~~~
cd /tmp/
wget http://noc.ws.nsrc.org/downloads/nfdump_1.6.6-1_i386.deb
wget http://noc.ws.nsrc.org/downloads/nfdump-flow-
tools_1.6.6-1_i386.deb
~~~~~~
~~~~~~~

Installation:

~~~~~~
~~~~~~~
sudo dpkg --install nfdump_1.6.6-1_i386.deb
sudo dpkg --install nfdump-flow-tools_1.6.6-1_i386.deb
~~~~~~
~~~~~~~

Test et installation de nfcapd et nfdump

~~~~~~
~~~~~~~
mkdir /tmp/nfcap-test
nfcapd -E -p 9001 -l /tmp/nfcap-test
~~~~~~
~~~~~~~

... au bout d'un certain temps, une série de flux devrait être
affichée
sur votre écran.
~~~~~~~

Arrêtez l'outil avec CTRL-C, et inspectez le contenu de /tmp/nfcap-test

```
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
~~~~~~~
$ ls -l /tmp/nfcap-test
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
~~~~~~~
```

Vous devriez voir un ou plusieurs fichiers nommés nfcapd.2013xxyyzz

Inspectez ce(s) fichier(s) avec nfdump:

```
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
~~~~~~~
nfdump -r /tmp/nfcap-test/nfcapd.2013xxyyzz | less
nfdump -r /tmp/nfcap-test/nfcapd.2013xxyyzz -s srcip/bytes
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
~~~~~~~
```

Vous devriez y trouvez quelques informations utiles :)