% Supervision NetFlow
%
% Gestion et Surveillance de Réseau

Introduction

Objectifs

* Apprendre à exporter des flux depuis un routeur Cisco

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.

Exporter les flux depuis un routeur Cisco

Pendant cet exercice, on vous demande d'exporter les flux depuis
votre routeur vers deux PC dans la classe. Vous devez travaiiler
en groupe. C'est à dire, pour le groupe 1, les utilisateurs des
pc1, pc2, pc3 et pc4 doivent travailler ensemble, et choisir une
machine sur laquelle les flux arriveront.

Par ailleurs, vous exporterez un second flux depuis le routeur
de votre groupe, vers le groupe voisin du vôtre. Par exemple, si
vous êtes dans le groupe 1, et si le groupe 2 a désigné le pc5 comme
celui
qui recevra les flux, alors vous configurerez votre routeur pour
qu'il
utilise pc5 comme seconde destination pour les flux.

Et si vous choisissez pc1 pour recevoir les flux de votre routeur
(rtr1),
alors il devra également recevoir des flux du routeur 2 (rtr2).

Pour résumer:

```
Group 1, Routeur 1
------------------
rtr1 ==> pc1 port 9001
rtr1 ==> pc5 port 9002

Group 2, Routeur 2
------------------
rtr2 ==> pc5 port 9001
rtr2 ==> pc1 port 9002

Choisir la meilleure combinaison pour vos groupes.

On peut faire ça de la manière suivante:

* groupes 1 et 2
* groupes 3 et 4
* groupes 5 et 6
* groupes 7 et 8

Si il y a un groupe 9, voyez avec les instructeurs.

Si vous avez 3 groupes, on peut faire:

rtr1 ==> pc1 port 9001
rtr1 ==> pc5 port 9001

rtr2 ==> pc5 port 9002
rtr2 ==> pc9 port 9001

rtr3 ==> pc9 port 9002
rtr3 ==> pc1 port 9002

... la règle étant:

- chaque routeur doit exporter vers deux destination: une dans votre
groupe,
  une dans un autre groupe

- chaque PC désigné dans le groupe reçoit deux flux: un de votre
groupe, et
  un depuis un autre groupe

Configuration:

~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
~~~~~~~
$ ssh cisco@rtr1.ws.nsrc.org
```

```
rtr1.ws.nsrc.org> enable
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
~~~~~~~

Si ssh n'est pas encore activé:

~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
~~~~~~~
$ telnet 10.10.1.254
Username: cisco
Password:
Router1>enable
Password:
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
~~~~~~~

Rappel - ceci est un EXEMPLE pour le cas suivant - à vous d'adapter!

rtr1 ==> pc1 on port 9001
rtr1 ==> pc5 on port 9002

Les autres groupes (2,3,4,5,6,7,8,9) feront différemment.

La section suivante active l'export des flux sur l'interface
FastEthernet 0/0.

~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
~~~~~~~
rtr1.ws.nsrc.org# configure terminal
rtr1.ws.nsrc.org(config)# interface FastEthernet 0/0
rtr1.ws.nsrc.org(config-if)# ip flow ingress
rtr1.ws.nsrc.org(config-if)# ip flow egress
rtr1.ws.nsrc.org(config-if)# exit
rtr1.ws.nsrc.org(config)# ip flow-export destination 10.10.1.1 9001
rtr1.ws.nsrc.org(config)# ip flow-export destination 10.10.2.5 9002
rtr1.ws.nsrc.org(config)# ip flow-export version 5
rtr1.ws.nsrc.org(config)# ip flow-cache timeout active 5
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
~~~~~~~

Ceci découpe les flux de long durée en fragments de 5 minute. Vous
pouvez choisir n'importe quel intervalle de temps entre 1 et 60
minutes. Si vous laissez la valeur par défaut de 30 minutes, vos
graphes auront des pics de traffic.

~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
~~~~~~~
```

```
rtr1.ws.nsrc.org(config)# snmp-server ifindex persist
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
~~~~~~~
```

Ceci active la persistence des index SNMP de vos interfaces. C'est pour
garantir que les valeurs de ifIndex ne changent pas si vous ajoutez ou supprimez des modules interface à vos équipements réseau.

Maintenant, configurons les paramètres de ip flow top-talkers:

```
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
~~~~~~~
rtr1.ws.nsrc.org(config)#ip flow-top-talkers
rtr1.ws.nsrc.org(config-flow-top-talkers)#top 20
rtr1.ws.nsrc.org(config-flow-top-talkers)#sort-by bytes
rtr1.ws.nsrc.org(config-flow-top-talkers)#end
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
~~~~~~~
```

On va maintenant vérifier ce qu'on à fait:

```
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
~~~~~~~
rtr1.ws.nsrc.org# show ip flow export
rtr1.ws.nsrc.org# show ip cache flow
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
~~~~~~~
```

Notez la distribution de la taille des paquets. Quel sont les deux tailles de paquets les plus présentes ?

See your "top talkers" across your router interfaces

```
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
~~~~~~~
rtr1.ws.nsrc.org# show ip flow top-talkers
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
~~~~~~~
```

Si cela a l'air ok, alors écrire la configuration running-config dans
la NVRAM (c'est à dire la configiration de démarrage):

```
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
~~~~~~~
rtr1.ws.nsrc.org#wr mem
```

~~~~~~

Vous pouvez maintenant quitter le routeur:

```
rtr1.ws.nsrc.org#exit
```

Vérifier que les flux arrivent bien depuis votre routeur, jusqu'au PC
désigné pour recevoir les flux dans votre groupe.

```
$ sudo tcpdump -Tcnfp port 9001
```

Attendez quelques secondes, et vous devriez voir quelque chose ressemblant
à ceci:

```
06:12:00.953450 IP s2.ws.nsrc.org.54538 > noc.ws.nsrc.org.9009:
NetFlow v5, 9222.333 uptime, 1359871921.013782000, #906334, 30 recs
  started 8867.952, last 8867.952
    10.10.0.241/0:0:53 > 10.10.0.250/0:0:49005 >> 0.0.0.0
    udp tos 0, 1 (136 octets)
  started 8867.952, last 3211591.733
    10.10.0.241/10:0:0 > 0.0.0.0/10:0:4352 >> 0.0.0.0
    ip tos 0, 62 (8867952 octets)
[...]
```

Si vous utilisez Netflow v9, notez que l'exemple ci-dessus ne sera pas
identique, comme la version de tcpdump dans Ubuntu ne décode pas toujours
correctement le Netflow v9.

Vérifier que les flux venant du routeur de votre groupe voisi arrivent
bien sur le PC désigné pour recevoir les flux dans VOTRE groupe (il faut
attendre que ceux-ci soient prêts et que l'export des flux soit activé):
~~~~~~

~~~~~~
$ sudo tcpdump -Tcnfp port 9002
~~~~~~

Ce labo est terminé.

Maintenant, allons faire l'exercice 2 exercise2-install-nfdump-nfsen.