% Monitorización de Netflow con NFSen
%
% Gestión de Redes

Introducción

Metas

* Aprender a exportar flujos desde un enrutador Cisco

Notas

* Los comandos precedidos por "$" implican que debe ejecutar el comando como usuario genérico - no como root
* Los comandos precedidos por "#" implican que deber· estar trabajando como usuario root.
* Los comandos con inicios de li≠nea m·s específicos como "rtrX>" o "mysql>" indican que debe ejecutar los comandos en un equipo remoto, o dentro de otro programa.

Exportar flujos desde un enrutador Cisco

Deber· trabajar en parejas. O sea, para el grupo 1, los usuarios de los pc1 y Pc2 y para el otro grupo deberan ser los usuarios de los pc3 y pc4. (Si sÛlo hay tres personas en su grupo, entonce tercera persona va a hacer todo por sí mismo.

Debido a que su router Cisco sólo puede exportar flujos a dos destinos al mismo tiempo, vamos a utilizar la siguiente configuración:

Grupo 1, Router 1
----

    rtr1 ==> pc1 on port 9001
    rtr1 ==> pc3 on port 9001

Grupo 2, Router 2
----

    rtr2 ==> pc5 on port 9001
    rtr2 ==> pc7 on port 9001

etc. Por lo tanto los flujos sólo llegar·n a la primera PC en cada pareja. Sin embargo, cuando s instala nfsen, ambas personas pueden apuntar su navegador web a la primera PC.

Configurar los Routers

~~~~~~
$ ssh cisco@rtrX.ws.nsrc.org
rtrX> enable
~~~~~~

o, si ssh no esta configurado todavia:

~~~~~~
$ telnet rtrX.ws.nsrc.org
Username: cisco
Password:
Router1>enable
Password:

A continuacion configura la interfaz FastEthernet 0/0 para exportar los flujos.
~~~~~~

Reemplace 10.10.XY con la dirección IP de la PC en tu par que va a recibirlos.

```
rtrX# configure terminal
rtrX(config)# interface FastEthernet 0/0
rtrX(config-if)# ip flow ingress
rtrX(config-if)# ip flow egress
rtrX(config-if)# exit
rtrX(config)# ip flow-export destination 10.10.X.Y 9001
rtrX(config)# ip flow-export destination 10.10.X.Z 9001
rtrX(config)# ip flow-export version 5
rtrX(config)# ip flow-cache timeout active 5
```

El ultimo comando particiona los flujos de larga duración en fragmentos de 5 minutos. Usted pued elegir el n˙mero de minutos entre el 1 y el 60. Si lo deja en el valor por defecto de 30 minutos los informes de tráfico tendrán picos.

```
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
rtrX(config)# snmp-server ifindex persist
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
```

Esto asegura que los indices SNMP se conserven durante el reinicio del router - También si añade elimina módulos de interfaz para los dispositivos de red.

Ahora configure cómo quiere que los top-talkers funcionen:

```
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
rtrX(config)# ip flow-top-talkers
rtrX(config-flow-top-talkers)# top 20
rtrX(config-flow-top-talkers)# sort-by bytes
rtrX(config-flow-top-talkers)# end
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
```

Ahora verificaremos lo que hemos hecho:

```
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
rtrX# show ip flow export
rtrX# show ip cache flow
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
```

Observe la distribución de tamaño de paquete - cuáles son los dos tamaños de paquete más comunes

Vea los "top talkers" para las diferentes interfaces

```
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
rtrX# show ip flow top-talkers
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
```

Si todo parece estar bien, guarde su configuraciÛn:

```
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
rtrX# write mem
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
```

Puede salir del enrutador:

```
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
rtrX# exit
```

~~~~~~

Compruebe que los flujos llegan a la PC elegida para recibir en su grupo:

~~~~~~
$ sudo tcpdump -v udp port 9001
~~~~~~

Espere unos segundos y deber√≠a ver algo como sigue:

```
06:12:00.953450 IP s2.ws.nsrc.org.54538 > noc.ws.nsrc.org.9009: NetFlow v5, 9222.333 uptime, 135
  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)
[...]
```

Estos son los paquetes UDP que contienen registros de flujo individuales.

Si est· utilizando Netflow v9, tenga en cuenta que la salida anterior puede no estar correcta, c
tcpdump en esta versión de Ubuntu no decodifica Netflow v9 correctamente.

Verifique que los flujos están llegando desde el enrutador del grupo contiguo a la PC elegida en
grupo para recibir flujos (puede que tenga que esperar a que el grupo vecino termine de configur
la exportación)

~~~~~~
$ sudo tcpdump -v udp port 9002
~~~~~~

Cuando esta seguro que los Flujos estan llegando puede seguir con el segundo ejercicio.
~~~~~~