Monitoring Netflow with NFsen (Part 1)

Introduction

The purpose of this exercise is to learn how to configure netflow on the campus Border router. We will use the existing campus network we have built.

Export flows from a Cisco router

This is an example for doing this from the **Campus X** border router, bdr1-campusX, to the PC named pc1-campusX.ws.nsrc.org. In each of your groups 1 to 6 you must choose one person to type in the commands to set up your border router for Netflow and the management server where the Netflow exports will go.

Configuring the flow exporter

Login to the border router and enter configuration mode.

First of all we will set up a flow exporter on the border router - this defines where we are going to export the flow information we have gathered from the router.

```
! Configuration for your BORDER router only
flow exporter EXPORTER-1
  description Export to VM
  destination 100.68.X.130
  transport udp 900X
  template data timeout 60
!
```

Replace the **X** with your campus number.

Configuring the flow monitor

Next we will set up the flow monitors - we will set up one for IPv4 and another for IPv6. These monitors let us monitor what is happening on the chosen interface of the border router.

```
flow monitor FLOW-MONITOR-V4
  exporter EXPORTER-1
  record netflow ipv4 original-input
  cache timeout active 300
!
```

```
flow monitor FLOW-MONITOR-V6
  exporter EXPORTER-1
  record netflow ipv6 original-input
  cache timeout active 300
!
```

Attaching the flow monitor to an interface

Finally we will configure the FastEthernet 0/1 interface with the monitors we have created. Substitute X with your group number.

```
interface FastEthernet 0/1
 ip flow monitor FLOW-MONITOR-V4 input
 ip flow monitor FLOW-MONITOR-V4 output
 ipv6 flow monitor FLOW-MONITOR-V6 input
 ipv6 flow monitor FLOW-MONITOR-V6 output
!
```

Why are we applying this to the 0/1 (inside) interface? So that our Netflow records show the internal addresses before they are NAT'd.

Since you have not specified a protocol version for the exported flow records, you get the default which is Netflow v9.

The “cache timeout active 300” command breaks up long-lived flows into 5-minute fragments. If you leave it at the default of 30 minutes your traffic reports will have spikes.

Also make sure that the following command is still present on the border router:

```
snmp-server ifindex persist
```

This enables ifIndex persistence globally. This ensures that the ifIndex values are retained during router reboots - also if you add or remove interface modules to your network devices.

Confirmation tools

Now we'll verify what we've done. Exit configuration mode, save the configuration, and then use these commands:

```
show flow exporter EXPORTER-1
show flow monitor FLOW-MONITOR-V4
```

It's possible to see the individual flows that are active in the router:

```
show flow monitor FLOW-MONITOR-V4 cache
```

But on a busy router there will be thousands of individual flows, so that's not useful. Press 'q' to escape from the screen output if necessary.

Instead, group the flows so you can see your “top talkers” (traffic destinations and sources). This is one very long command line:

```
show flow monitor FLOW-MONITOR-V4 cache aggregate ipv4 source address ipv4
       destination address sort counter bytes top 50
```

You can do the same for IPv6:

```
show flow monitor FLOW-MONITOR-V6 cache aggregate ipv6 source address ipv6
      destination address sort counter bytes top 50
```

In fact, this command is so long, it is a lot to type each time you want to find out the top 50 most active flows. So most network operators create a command alias, like the two below. Enter into configuration mode to set these two up on the border router:

```
alias exec top-v4talkers show flow monitor FLOW-MONITOR-V4 cache aggregate
ipv4
      source address ipv4 destination address sort counter bytes top 50
alias exec top-v6-talkers show flow monitor FLOW-MONITOR-V6 cache aggregate
ipv6
      source address ipv6 destination address sort counter bytes top 50
```

Once you have set up the alias, you can simply enter “top-v4talkers” and “top-v6talkers” at the command prompt to find out the top 50 IPv4 and IPv6 flows on the border router.

See the flows on the NMS PC

Now login to your monitoring server, pc1-campusX.ws.nsrc.org, using ssh. To check flow packets are arriving here, you can use tcpdump:

```
$ sudo apt-get install tcpdump
$ sudo tcpdump -i eth1 -nn udp port 900X
```

Wait a few seconds and you should see packets arriving. These are the UDP packets containing individual flow records, but you won't be able to read the contents.

Because your campus doesn't have any real users on it, it might take a while before you see flows, so you might need to generate some traffic in your campus. One way is to get some other people in your group to login to pc1-campusX.ws.nsrc.org (with ssh) and disconnect a few times.