Monitoring Netflow with NfSen

Contents

1 Introduction

1.1 Goals

- Learn how to export flows from a Cisco router

1.2 Notes

- Commands preceded with “$” imply that you should execute the command as a general user - not as root.
- Commands preceded with “#” imply that you should be working as root.
- Commands with more specific command lines (e.g. “rX1>” or “mysql>”) imply that you are executing commands on remote equipment, or within another program.

2 Export flows from a Cisco router

You will configure your router to export the same flow data to all PCs in your group.

2.1 Group 1, Router 1

vm rX1 ==> vm1 on port 9001 rX1 ==> vm2 on port 9001 rX1 ==> vm3 on port 9001 rX1 ==> vm4 on port 9001

2.2 Group 2, Router 2

```
rtr2 ==> vm7 on port 9001
rtr2 ==> vm8 on port 9001
rtr2 ==> vm9 on port 9001
rtr2 ==> vm10 on port 9001
```

etc.

3 Configuring the routers

```
$ ssh nsrc@rX1.ws.nsrc.org
rX1> enable
```

or, if ssh is not configured yet:

```
$ telnet 10.10.1.254
Username: nsrc
Password:
Router1>enable
Password:
```

The following configures the FastEthernet 0/0 interface to export flows. Replace 10.10.X.A to .D with the IP addresses of the PCs in your group.

```
rX1# configure terminal
rX1(config)# flow exporter EXPORTER-1
rX1(config-flow-exporter)# description Export to vmA
rX1(config-flow-exporter)# destination 10.10.X.A
rX1(config-flow-exporter)# transport udp 9001
rX1(config-flow-exporter)# template data timeout 300
```

```
... repeat for EXPORTER-2 and vmB
... repeat for EXPORTER-3 and vmC
... repeat for EXPORTER-4 and vmD
rX1(config-flow-exporter)# flow monitor FLOW-MONITOR-V4
rX1(config-flow-monitor)# exporter EXPORTER-1
rX1(config-flow-monitor)# exporter EXPORTER-2
rX1(config-flow-monitor)# exporter EXPORTER-3
rX1(config-flow-monitor)# exporter EXPORTER-4
rX1(config-flow-monitor)# record netflow ipv4 original-input
rX1(config-flow-monitor)# cache timeout active 300
rX1(config)# interface FastEthernet 0/0
rX1(config-if)# ip flow monitor FLOW-MONITOR-V4 input
rX1(config-if)# ip flow monitor FLOW-MONITOR-V4 output
rX1(config-if)# exit
```

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.

> Aside: to monitor IPv6 flows you would have to create a new flow monitor for IPv6 and attach it to the interface and the existing exporters.
>
> ```
> flow monitor FLOW-MONITOR-V6
>  exporter EXPORTER-1
>  exporter EXPORTER-2
>  exporter EXPORTER-3
>  exporter EXPORTER-4
>  record netflow ipv6 original-input
>  cache timeout active 300
> interface FastEthernet 0/0
>  ipv6 flow monitor FLOW-MONITOR-V6 input
>  ipv6 flow monitor FLOW-MONITOR-V6 output
> ```

Also enter the following command:

```
rX1(config)# 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.

Now we’ll verify what we’ve done.

First exit from the configuration session:

```
rX1(config)# exit
```

```
rX1# show flow exporter EXPORTER-1
rX1# show flow exporter EXPORTER-2
etc...
rX1# show flow monitor FLOW-MONITOR-V4
```

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

```
rX1# show flow monitor FLOW-MONITOR-V4 cache
```

But 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:

```
rX1# show flow monitor FLOW-MONITOR-V4 cache aggregate ipv4 source address
      ipv4 destination address sort counter bytes top 20
```

If it all looks good then write your running-config to non-volatile RAM (i.e. the startup-config):

```
rX1#wr mem
```

You can exit from the router now:

```
rX1#exit
```

Make sure we have the tcpdump tool installed:

```
$ sudo apt-get install tcpdump
```

Now verify that flows are arriving from your router to your PC:

```
$ sudo tcpdump -i eth0 -nn -Tcnfp port 9001
```

Wait a few seconds and you should see something that looks like:

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

These are the UDP packets containing individual flow records.

(Note that the actual output may not be correct, as tcpdump does not decode Netflow properly)

3.1 Generating some traffic

Our lab setup doesn't really generate much traffic. We can create a bit of traffic by configuring ntp our routers and switches. On each of your devices:

```
conf t
ntp server 10.10.0.254
exit
wr mem
```

You are done for this lab.

Go to exercise2-install-nfdump-nfsen.