Monitoring Netflow with NFsen (Part 2)

Goals

- Learn how to export flows from a Cisco router
- Learn how to install the nfdump and NfSen tools
- Learn how to configure and use the Top Talkers feature

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. "rtrX>" or "mysql>") imply that you are executing commands on remote equipment, or within another program.

Configure Your Collector

Install NFDump and associated software

NFdump is part of the Netflow flow collector tools, which includes:

nfcapd, nfdump, nfreplay, nfexpire, nftest, nfgen

There is a package in Ubuntu, but it's too old - so we're going to build it from source. First, check you have the build tools and dependencies:

```
$ sudo apt-get update
$ sudo apt-get install build-essential autoconf
$ sudo apt-get install rrdtool mrtg librrds-perl librrdp-perl librrd-dev \
      libmailtools-perl php5 bison flex wget
```

When you are asked, "Make /etc/mrtg.cfg owned by and readable only by root?" you should answer <Yes>.

Now proceed to download and build. Note that only the last step (make install) has to be done as root.

```
$ cd
$ wget http://www.ws.nsrc.org/downloads/nfdump-1.6.13.tar.gz
$ tar xvzf nfdump-1.6.13.tar.gz
$ cd nfdump-1.6.13
$ ./configure --help      # optional, shows the build settings available
$ ./configure --enable-nfprofile --enable-nftrack
$ make
$ sudo make install
```

Testing nfcapd and nfdump

```
$ mkdir /tmp/nfcap-test
$ nfcapd -E  -p 900X -l /tmp/nfcap-test
```

Browse the web from your laptops which are in your "campus". After a while, a series of flows should be dumped on your screen.

Stop the tool with CTRL+C, then look at the contents of /tmp/nfcap-test

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

You should see one or more files called nfcapd.<YEAR><MON><DAY><HR><MIN>

Process the file(s) with nfdump:

```
nfdump -r /tmp/nfcap-test/nfcapd.201Ywwxxyyzz | less
nfdump -r /tmp/nfcap-test/nfcapd.201Ywwxxyyzz -s srcip/bytes
```

You should get some useful information :)

Installing and setting up NfSen

Download and compile. The patch is to fix a problem reported at
http://sourceforge.net/p/nfsen/bugs/31/

```
$ cd
$ wget http://www.ws.nsrc.org/downloads/nfsen-1.3.6p1.tar.gz
$ tar xvzf nfsen-1.3.6p1.tar.gz
$ cd nfsen-1.3.6p1
$ wget http://www.ws.nsrc.org/downloads/nfsen-socket6.patch
$ patch -p0 < nfsen-socket6.patch
$ cd etc
$ cp nfsen-dist.conf nfsen.conf
$ editor nfsen.conf
```

Set the \$BASEDIR variable

```
$BASEDIR = "/var/nfsen";
```

Set the users appropriately so that Apache can access files:

```
$WWWUSER = 'www-data';
$WWWGROUP = 'www-data';
```

Set the buffer size to something small, so that we see data quickly. You would not do this on a production system.

```
# Receive buffer size for nfcapd - see man page nfcapd(1)
$BUFFLEN = 2000;
```

Find the %sources definition, and change it to:

```
%sources=(
 'bdr1-campusX' => {'port'=>'900X','col'=>'#0000ff','type'=>'netflow'},
 );
```

(substitute your group number for **X**, and either remove or comment out the existing sample sources). Now save and exit from the file.

Finally, change the HTMLDIR from /var/www/nfsen/ to /var/www/html/nfsen/

```
$HTMLDIR    = "/var/www/html/nfsen/";
```

Create the netflow user on the system

```
$ sudo useradd -d /var/nfsen -G www-data -m -s /bin/false netflow
```

Install NfSen and start it

Change directory back to just inside the source directory:

```
$ cd
$ cd nfsen-1.3.6p1
```

Now, finally, we install:

```
$ sudo perl install.pl etc/nfsen.conf
```

Press ENTER when prompted for the path to Perl.

Install init script

In order to have nfsen start and stop automatically when the system starts, add a link to the init.d diretory pointing to the nfsen startup script:

```
$ sudo ln -s /var/nfsen/bin/nfsen /etc/init.d/nfsen
$ sudo update-rc.d nfsen defaults 20
```

Start NfSen

```
$ sudo service nfsen start
```

Check that nfcapd processes have been started:

```
$ ps auxwww | grep nfcapd
```

View flows via the web

You can find the nfsen page here:

```
http://pc1-campusX.ws.nsrc.org/nfsen/nfsen.php
```

Everyone in the group can point their web browser at this page.

You may see a message such as:

```
Frontend - Backend version mismatch!
```

This will go away if you reload the page, it's not a problem.

Done!! Show your working system to the workshop instructors.

Notes

Error messages

On some newer Linux distribution releases (Fedora Core 16 and above, Ubuntu 12.04 LTS and above, etc.) you may see error like this when starting nfsen:

```
Subroutine Lookup::pack_sockaddr_in6 redefined at
/usr/share/perl/5.14/Exporter.pm line 67.
at /var/nfsen/libexec/Lookup.pm line 43
```

nfsen will still load and function properly, so you can ignore this error for now (or solve the problem and give back to the nfsen project! 😀).

Adding sources

If you had multiple routers in your network all sending flows to the same collector, you can either configure them to send to different ports on the collector, or you can tell nfsen the source IP address of each router. This allows nfsen to show distinct data from each source.

DON'T DO THIS NOW as you only have a single router, but if you needed to, you would do it as follows:

Edit /var/nfsen/etc/nfsen.conf, and add the source(s), for example:

```
%sources = (
'r1-bdr-campus1' => {'port' => '9001', 'col' => '#e4e4e4' },
'r1-bdr-campus2' => {'port' => '9002', 'col' => '#0000ff' },
```

```
'r1-bdr-campus3' => {'port' => '9003', 'col' => '#00cc00' },
);
```

Reconfigure NfSen.

You will need to run this every time you modify /var/nfsen/etc/nfsen.conf:

```
$ sudo /etc/init.d/nfsen reconfig
```

You should see:

```
New sources to configure : bdr1-campus2 bdr1-campus3
Continue? [y/n] y

Add source 'bdr1-campus2'
Add source 'bdr1-campus3'

Start/restart collector on port '9002' for (bdr1-campus2)[pid]
Start/restart collector on port '9003' for (bdr1-campus3)[pid]

Restart nfsend:[pid]
```