Installation and configuration of NFSen and NFDump

- In this example I use Ubuntu 8.10

This document is a quick and dirty translation from my original Dutch document.
If you have any questions or comments, don’t hesitate to contact me.

Rob Maas rob@progob.nl

How it works

There are services(=daemons) that are started, they will listen on the listed ports to capture the xFlow data. There are two kind of daemons.

- nfcapd – Netflow capture daemon (it is mostly used on Cisco devices)
- sfcapd – sFlow capture daemon (for HP Procurve devices we need this one)

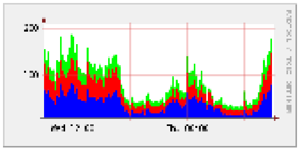
These daemons capture all the data and will save this data it to a directory.

The naming of the capture files will look like: “*nfcapd.200812110855*” this files can be printed in a readable format with the use of NFDump.

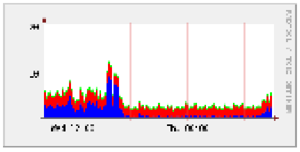
```
rob@pcndi0001:~/nfsen/profiles-data/live/SWDT10001A/2008/12/11$ nfdump -r ./nfcapd.200812110855 -c 10
Date flow start          Duration Proto      Src IP Addr:Port          Dst IP Addr:Port   Packets    Bytes Flows
2008-12-11 08:55:00.178     0.000 TCP           10.1.0.1:445   ->        10.1.0.40:2717       512   314880     1
2008-12-11 08:55:00.178     0.000 UDP         10.11.1.27:32560 ->       10.11.1.41:32688      512    92160     1
2008-12-11 08:55:00.178     0.000 TCP         10.1.0.106:1025  ->       10.1.0.107:35818      512    92160     1
2008-12-11 08:55:00.178     0.000 TCP         10.1.0.145:2598  ->       10.10.1.10:1051       512    92160     1
2008-12-11 08:55:00.178     0.000 TCP         10.1.0.145:2598  ->     10.153.11.25:1059       512    92160     1
2008-12-11 08:55:00.178     0.000 SRP         10.6.1.162:2598  ->        10.6.1.10:1059       512    92160     1
2008-12-11 08:55:00.178     0.000 TCP       10.153.11.37:1078  ->       10.1.0.152:2598       512    92160     1
2008-12-11 08:55:00.178     0.000 TCP          10.1.0.97:397   ->      10.138.10.1:20667      512    92160     1
2008-12-11 08:55:00.407     0.000 TCP          10.1.50.6:1433  ->         10.1.5.2:3557       512    38400     1
2008-12-11 08:55:00.407     0.000 TCP          10.1.50.3:445   ->        10.1.0.73:1324       512    40448     1
Summary: total flows: 10, total bytes: 1038848, total packets: 5120, avg bps: 34.6 M, avg pps: 22358, avg bpp: 202
Time window: 2008-12-11 08:55:00 - 2008-12-11 08:59:06
Total flows processed: 16132, Records skipped: 0, Bytes read: 838876
Sys: 0.000s flows/second: 0.0        Wall: 0.001s flows/second: 11019125.7
```

But, we all like pictures and this is where we use NFSen. NFSen uses the above tools to create nice graphs.

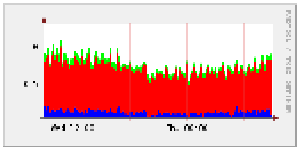
TCP



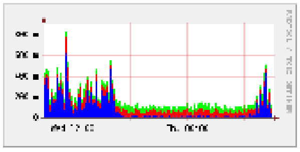
UDP

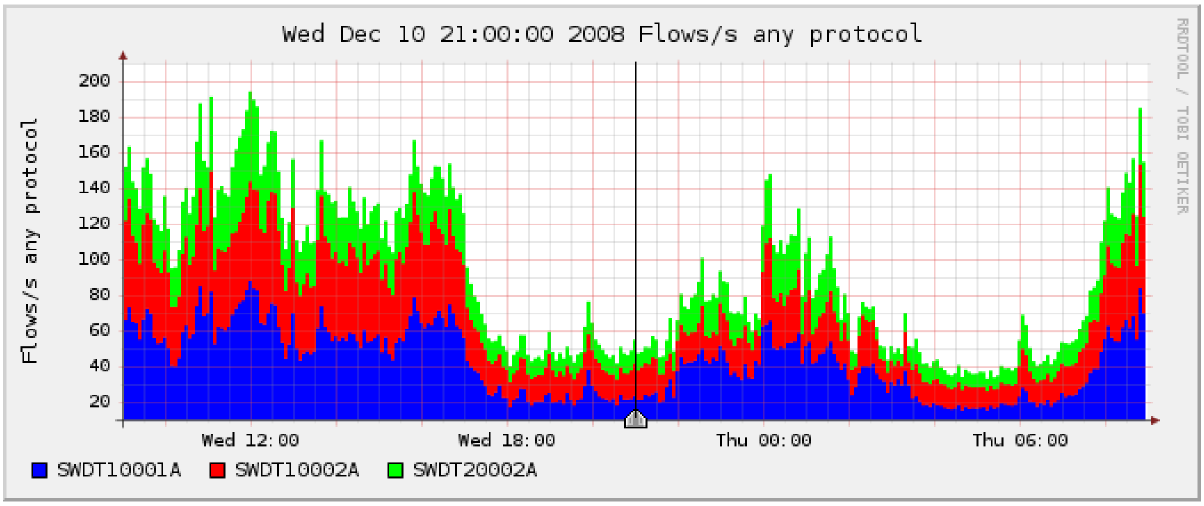


ICMP



other





Installation

NFDUMP

To be able to install NFDump we need some additional packages. These are easily installed with the following commands. If you like you can do this at once.

```
sudo apt-get install flex
sudo apt-get install rrdtool librrd2 librrd2-dev
sudo apt-get install perl-byacc
```

First we are going to download the software, just to keep things simple we put everything in the “home” folder. Go to the terminal and type “*cd ~/*”.

To download the tools, you can use the following command.

```
wget http://garr.dl.sourceforge.net/sourceforge/nfdump/nfdump-1.5.7.tar.gz
```

Use the following command to unzip and untar the file.

“*tar -xvf ./nfdump-1.5.7.tar.gz*”

Now we are going to the just unzipped directory with “*cd nfdump-1.5.7*”.
To prepare everything for the installation type.

```
./configure --enable-nfprofile --enable-sflow
```

The enable-nfprofile parameter is needed for NFSen and enable-sflow is needed to make sure sfcapd will be included.

After this we can start the real installation. With the following commands.

```
make
make install
```

Now NFDump is installed.

> ***Hint!*** *NFDump is also available in the repositories of Ubuntu, only the sflow daemon won’t be installed.*

NFSEN

NFSen is a web based application and to make sure we can run NFSen properly we need some addition packages. For example we need apache(web server) and we need PHP(to process the pages).

These packages are also easily installed by the following commands.

```
sudo apt-get install php5
sudo apt-get install librrds-perl
```

To make it easy once again we go to the home directory by typin "*cd ~/*".

NFSen has to be downloaded separate from NFDump, so use the following command to download NFSen.

```
wget http://dfn.dl.sourceforge.net/sourceforge/nfsen/nfsen-1.3b-20070824.tar.gz
```

After this also this package has to be unzipped.

```
tar -xvf ./nfsen-1.3b-20070824.tar.gz
```

We go to the directory with "*cd nfsen-1.3b-20070824*", before we change te configuration we make a copy of the original.

```
cp etc/nfsen-dist.conf etc/nfsen.conf
```

To edit the file type (of course you are free to use other editors as nano)

```
nano etc/nfsen.conf
```

The following options has to be configured.

The BASEDIR directory is the main directory where all the information is stored. I use the home directory.

```
$BASEDIR = "/home/rob/nfsen";
```

We also need to tell which user is used for NFSen. You can also make a dedicated NFSen user.

```
$USER    = "beheer";
```

Besides the NFSen user we need to tell NFSen who is the WWW user. In Ubuntu this is www-data by default.

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

One of the most important things is to tell NFSen which deamons need to be used.

```
%sources = (
    'upstream1'    => { 'port'    => '9995', 'col' => '#0000ff', 'type' => 'netflow' },
    'peer1'        => { 'port'    => '9996', 'col' => '#ff0000' },
);
```

You can change this to something like this.

```
%sources = (
    'SWITCH01'    => { 'port'    => '6343', 'col' => '#0000ff', 'type' => 'sflow' },
);
```

In this example I start a sflow capture on port 6343. For each deamon we need to configure a separate unique port. The #0000FF is the color we like to see in the graphs. This value is a RGB color in hex.

After you are done with the configuration. You can use CTRL+X to close nano, but before it will close it will ask you to save the configuration a simple “y” is enough.

Now we just have to take care that the NFSen user is a member of the www-data group. This can be easily done with the following command.

sudo usermod -G www-data beheer

Now we are done with the configuration we can install NFSen.

sudo ./install.pl etc/nfsen.conf

After setup it is recommended to restart apache.

/etc/init.d/apache2 restart

After this we start NFSen.

sudo ~/nfsen/bin/nfsen start

If everything went fine, we can now access NFSen with a webbrowser by going to the IP address of the server, followed by nfsen/nfsen.php.(http://ipserver/nfsen/nfsen.php)

Switch configuration (HP Procurve 5400)

Now we have the capture daemons running, but the switch is it sending is data to the daemon. To solve this we need to activate sflow (netflow) on the switch.

Telnet to the switch and go to the configuration mode.

Type the following command.

sflow 1 destination IPADDRESS PORT

With the configuration above, the daemon is capturing on port 6343, so this is the port we need to fill in. The IPADDRESS is the ip of the NFSen server.

You also need to tell the switch which ports you will capture, we choose for all.

sflow 1 polling ethernet all 20
sflow 1 sampling ethernet all 512

Below is a table with the best sample rates. (see: http://www.inmon.com)

	Traffic level		
Speed	**Low**	**Medium**	**High**
10 Mb/s	64	128	256
100 Mb/s	128	256	512
1Gb/s	256	512	1024
10Gb/s	512	1024	2048