Installatie en configuratie NFDump & NFSen

Voorbereiding

- Er wordt uitgegaan van een Ubuntu 8.10 als OS.
- Internettoegang beschikbaar.
- Zorg dan ook dat deze is geïnstalleerd en up-to-date.*
- SSH toegang kan configuratie vergemakkelijken **

** Updaten Ubuntu achter proxy*

- *Proxy instellen:* export http_proxy=”gebruiker:wachtwoord@server:poort”
- *Repositorie updaten:* sudo apt-get update
- *Systeem upgraden:* sudo apt-get upgrade

** * Tip: zorg voor SSH access (*sudo apt-get install openssh-server*), dan kun je remote m.b.v. bijv. Putty het systeem configureren.*

Werking

Het systeem werkt als volgt.

Er worden services(=deamons) opgestart die op een bepaalde poort luisteren voor xFlow pakketjes. Er zijn twee type deamons.

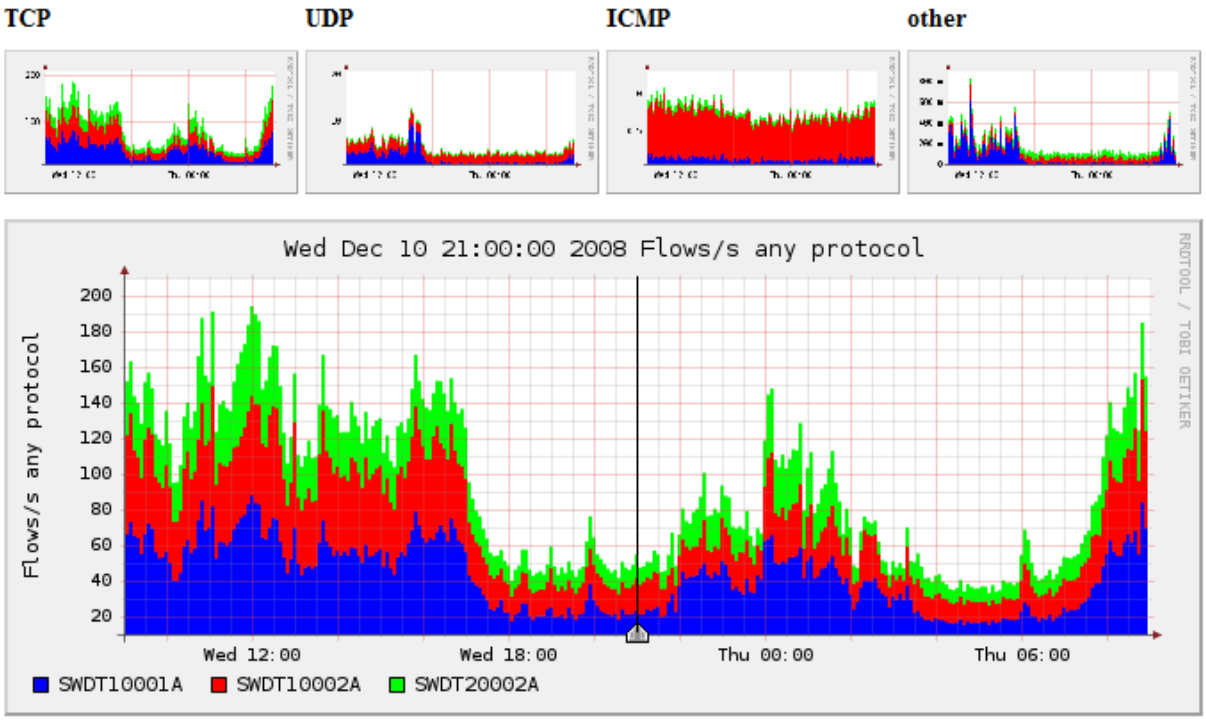
- nfcapd – NetFlow capture deamon (bijv. Cisco apparaten)
- sfcapd – sFlow capture deamon (bijv. HP Procurve apparaten)

Deze capture deamons, slaan alle gegevens op in (evt. opgegeven) een directory.

Een pakketje met een capture kan er zo uitzien: "*nfcapd.200812110855*" Deze pakketjes kunnen m.b.v. NFDump uitgelezen worden.

```
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
```

Echter zijn we allemaal dol op plaatjes en hier komt NFSen om de hoek kijken, NFSen gebruikt de bovengenoemde programma's, echter maakt deze mooie grafieken.



Installatie

NFDUMP

Om NFDump te kunnen installeren en gebruiken zijn er een aantal extra pakketten benodigd, deze kun je installeren met de onderstaande commando's, kan evt. ook in een keer.

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

Allereerst gaan we de software downloaden, dit doen we voor het gemak in de "home" directory van de gebruiker. Via de terminal doe je dit door "*cd ~/*" in te tikken.

Het downloaden kan met het volgende commando*

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

Hier kun je met "*ls*" zien wat er in je directory staat.
Met het commando "*tar -xvf ./nfdump-1.5.7.tar.gz*" pak je het net gedownload pakket uit.

Vervolgens gaan we naar de directory m.b.v. "*cd nfdump-1.5.7*", vervolgens kun je weer met "*ls*" in de directory kijken.

Nu voeren we de volgende opdracht uit, om alles klaar te zetten.

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

De enable-nfprofile is benodigd voor een correcte werking met NFSen en de enable-sflow is om ervoor te zorgen dat sfcapd meegenomen wordt.

Na de configuratie kunnen gaan we het pakket daadwerkelijk installeren, dit doen we met de volgende commando's.

make
make install

Nu is NFDump geïnstalleerd.

***Tip!** NFDump bevind zich ook in de softwarebronnen van Ubuntu, echter wordt hiermee niet de SFlow deamon sfcapd geïnstalleerd.*

** Het downloaden kan ook via de website: http://nfdump.sourceforge.net*
Downloaden met wget kan via de proxy m.b.v. de volgende parameters –proxy-user="user" –proxy-password="pass"

NFSEN

NFSen is een webgebaseerde applicatie en hiervoor zijn er een aantal pakketten nodig om dit allemaal goed te laten verlopen, denk hierbij bijv. aan apache (webserver) en PHP (om de pagina's op te bouwen).

Deze pakketten kunnen we met de volgende commando's installeren.
Sudo apt-get install php5
sudo apt-get install librrds-perl

Om het ons gemakkelijk te maken gaan we eerst naar de "home" directory, dit doen we m.b.v. het volgende commando "*cd ~/*".

NFSen moeten we los van NFDump downloaden en dit kan met het volgende commando *

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

Hierna moeten we ook dit pakketje uitpakken, dit kan met het volgende commando.

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

Vervolgens gaan we met "*cd nfsen-1.3b-20070824*" naar de directory.
Om de configuratie te maken, maken we eerst een kopie van het origineel.

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

Nu kunnen we zonder zorgen het configuratie bestand wijzigen.

nano etc/nfsen.conf

Zaken die ingesteld moeten worden:

De BASEDIR is de directory waar alles opgeslagen moet worden, momenteel gebruik ik hier de home directory voor.

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

Ook wordt de NFSen gebruiker gevraagd, echter kun je natuurlijk ook een aparte gebruiker aanmaken.

```
$USER    = "rob";
```

Naast deze gebruiker, moet ook de WWW gebruiker opgegeven worden, voor Ubuntu is dit standaard www-data, uiteraard is ook hiervoor de mogelijkheid dit aan te passen.

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

Verder is het ook belangrijk om de deamon informatie in te vullen.

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

Dit zou bijv. zo kunnen worden

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

Hier wordt er een sflow capture gestart op poort 6343. Voor elke deamon, moet er een aparte poort worden gespecificeerd. De #0000FF, geeft de kleur aan, RGB in hexadecimale waarden. Je kunt na de wijzigingen het bestand opslaan door op CTRL+X te drukken en vervolgens voor “y”es te kiezen.

Ook moet onze NFSen gebruiker zie boven lid zijn van de www-data groep, dit kunnen we met het onderstaande commando bereiken.

sudo usermod -G www-data beheer

Nu alles is geconfigureerd, kunnen we nfsen installeren.

sudo ./install.pl etc/nfsen.conf

Na de setup is het verstandig om de apache service te herstarten, dit kan met:

/etc/init.d/apache2 restart

Nu kunnen we nfsen starten.

sudo ~/nfsen/bin/nfsen start

Nu kun je via de webbrowser http://ipserver/nfsen/nfsen.php bereiken.

***Tip!** In het nfsen.conf kunnen nog veel meer wijzigingen worden aangebracht!*

** Het downloaden kan ook via de website: http://sourceforge.net/projects/nfsen/*

Switch configuratie (HP Procuve 5400)

Nu de deamon draait, moeten we zorgen dat de switch zijn flow data naar de deamon stuurt. Log in op de switch en zorg dat je in configuratie mode zit.

Tik het volgende in:

sflow 1 destination IPADRES POORT

Met de configuratie van net, zou de poort 6343 zijn, het ip-adres is het adres van de server die we net klaargemaakt hebben.

Als laatste moeten we nog kiezen welke poorten we meenemen, hiervoor stellen we polling en sampling in.

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

In plaats van ethernet all kun je ook de poorten los opgeven.

De beste sampling rates volgens 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