1) Réalisation d’une maquette Netflow sur la salle

1.1) Configuration de la sonde fprobe

IP de notre VM : 10.202.0.137

Pour commencer on installe fprobe :

```
apt-get install fprobe
```

Maintenant on configure le fichier /etc/default/fprobe de cette façon :

```
#fprobe default configuration file

INTERFACE="eth0"
FLOW_COLLECTOR="10.202.0.144:1561 10.202.0.168:1561 10.202.0.137:1561
10.202.0.94:1561 10.202.0.96:1561 10.202.0.64:1561
10.202.14.1:1561 10.202.0.66:1561 10.202.0.161:1561
10.202.0.73:1561 10.202.0.161:1561 10.202.0.175:1561"

#fprobe can't distinguish IP packet from other (e.g. ARP)
OTHER_ARGS="-fip"
```

Dans le fichier, l'adresse 10.202.0.137 est l'@IP de la machine virtuelle sur laquelle est configurée fprobe et on y a ajouté le port 1561. Nous devions commencer à 1155 mais nous ne devions pas avoir le même port que les autres membres de la classe. Pour toutes les autres IP des autres groupes il faut toujours mettre notre port à la fin

Une fois le fichier configuré on relance fprobe de la façon suivante :

```
systemctl stop fprobe
systemctl start fprobe
```

1.2) Configuration de nfsen

On commence par récupérer sur le git du prof le docker :

```
git clone https://registry.iutbeziers.fr:5443/pouchou/nfsen-dockerized.git
```

Une fois le docker récupéré on se déplace dans le répertoire crée

On vérifie que la date soit bonne sinon on la modifie de la façon suivante :

1. On va sur la machine physique et on fait la commande dpkg-reconfigure tzdata (on met Europe puis Paris)
2. Maintenant on se déplace dans le dossier du contrainer et on fait docker-compose stop
3. On termine par la commande docker-compose start

Maintenant on fait la commande suivante pour lancer l'application :

```
root@debian:~/nfsen-dockerized# docker-compose up -d
```

On peut à présent aller vérifier sur internet que nfsen est accessible sur le port 6080. Pour cela on met en URL "@IP de la VM:6080/nfsen"

On voit bien une page avec des graphes apparaître ce qui veut dire qu'il est accessible

On lance maintenant le docker :

```
docker-compose exec nfsen bash
```

On se déplace dans /data/nfsen/etc et on édite le fichier nfsen.conf de la façon suivante :

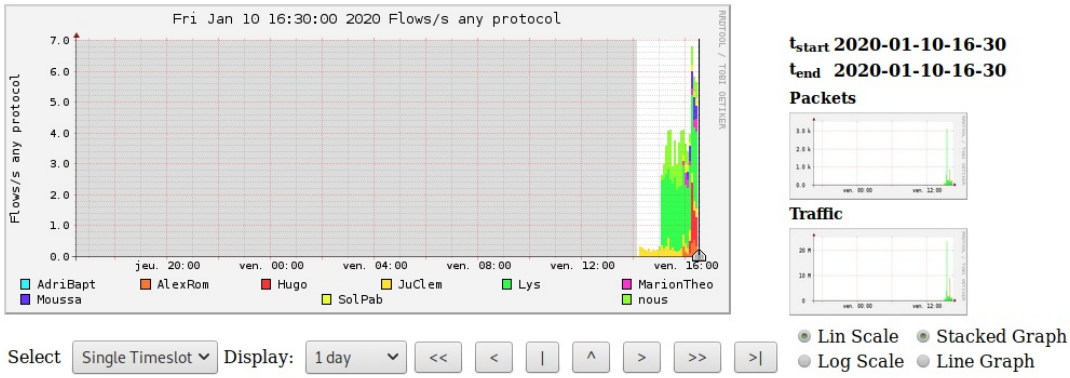
```
%sources = (
'nous' => {'port'=>'1561','col'=>'#8DFF33','type'=>'netflow'},
'AdriBapt' => {'port'=>'1558','col'=>'#33F3FF','type'=>'netflow'},
'Moussa' => {'port'=>'1557','col'=>'#6833FF','type'=>'netflow'},
'Hugo' => {'port'=>'1563','col'=>'#FF333C','type'=>'netflow'},
'SolPab' => {'port'=>'1564','col'=>'#E9FF33','type'=>'netflow'},
'JuClem' => {'port'=>'1565','col'=>'#FFE333','type'=>'netflow'},
'MarionTheo' => {'port'=>'1569','col'=>'#FF33D1','type'=>'netflow'},
'AlexRom' => {'port'=>'1572','col'=>'#FF7733','type'=>'netflow'},
'Lys' => {'port'=>'1573','col'=>'#33FF4F','type'=>'netflow'},
);
```

Maintenant on reconfigure nfsen et on obtient la chose suivante :

```
root@nfsen:/data/nfsen/etc# /data/nfsen/bin/nfsen reconfig
Start/restart collector on port '1565' for (JuClem)[306]
Start/restart collector on port '1561' for (nous)[309]
Start/restart collector on port '1558' for (AdriBapt)[312]
Start/restart collector on port '1573' for (Lys)[315]
Start/restart collector on port '1557' for (Moussa)[318]
Start/restart collector on port '1572' for (AlexRom)[321]
Start/restart collector on port '1569' for (MarionTheo)[324]
Start/restart collector on port '1563' for (Hugo)[327]
Start/restart collector on port '1564' for (SolPab)[330]

Restart nfsend:[34]
```

Maintenant on attend une quinzaine de minutes on devrait visualiser des graphes sur le navigateur :



Statistics timeslot Jan 10 2020 - 16:30

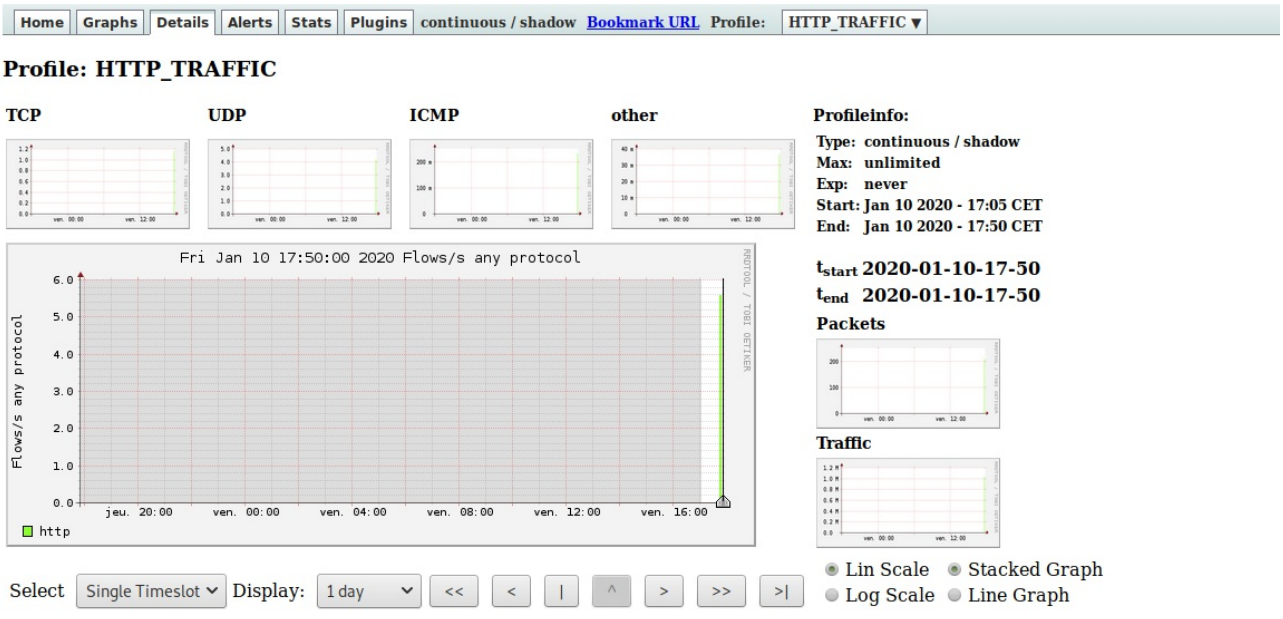
Channel:	Flows:					Packets:					Traffic:				
	all:	tcp:	udp:	icmp:	other:	all:	tcp:	udp:	icmp:	other:	all:	tcp:	udp:	icmp:	other:
nous	0.3 /s	0.1 /s	0.2 /s	0.0 /s	0.0 /s	4.3 /s	0.9 /s	3.1 /s	0.3 /s	0.0 /s	13.6 kb/s	7.4 kb/s	5.6 kb/s	543.1 b/s	10.7 b/s
SolPab	0.3 /s	0.2 /s	0.1 /s	0.1 /s	0.0 /s	9.3 /s	4.8 /s	2.2 /s	2.2 /s	0.0 /s	26.7 kb/s	20.5 kb/s	4.5 kb/s	1.7 kb/s	5.3 b/s
Moussa	0.5 /s	0.3 /s	0.2 /s	0.0 /s	0.0 /s	9.7 /s	5.4 /s	2.0 /s	2.3 /s	0.0 /s	16.5 kb/s	10.4 kb/s	4.1 kb/s	1.9 kb/s	5.3 b/s
MarionTheo	0.2 /s	0.0 /s	0.2 /s	0.0 /s	0.0 /s	3.7 /s	1.4 /s	2.1 /s	0.1 /s	0.0 /s	5.9 kb/s	1.7 kb/s	4.1 kb/s	96.0 b/s	5.3 b/s
Lys	1.9 /s	0.3 /s	1.5 /s	0.1 /s	0.0 /s	169.0 /s	154.4 /s	12.3 /s	2.3 /s	0.0 /s	890.7 kb/s	866.3 kb/s	21.9 kb/s	2.5 kb/s	1.1 b/s
JuClem	0.2 /s	0.0 /s	0.1 /s	0.0 /s	0.0 /s	2.8 /s	0.1 /s	2.3 /s	0.3 /s	0.0 /s	5.3 kb/s	57.2 b/s	4.6 kb/s	656.2 b/s	5.3 b/s
Hugo	0.2 /s	0.0 /s	0.2 /s	0.0 /s	0.0 /s	4.7 /s	1.2 /s	3.3 /s	0.1 /s	0.0 /s	8.0 kb/s	977.5 b/s	6.8 kb/s	161.3 b/s	10.7 b/s
AlexRom	0.1 /s	0.0 /s	0.1 /s	0.0 /s	0.0 /s	3.8 /s	1.6 /s	2.1 /s	0.1 /s	0.0 /s	5.7 kb/s	1.7 kb/s	3.8 kb/s	180.5 b/s	5.3 b/s
AdriBapt	0 /s	0 /s	0 /s	0 /s	0 /s	0 /s	0 /s	0 /s	0 /s	0 /s	0 b/s	0 b/s	0 b/s	0 b/s	0 b/s
	all:	tcp:	udp:	icmp:	other:	all:	tcp:	udp:	icmp:	other:	all:	tcp:	udp:	icmp:	other:
TOTAL	3.9 /s	0.9 /s	2.6 /s	0.3 /s	0.0 /s	207.1 /s	169.8 /s	29.5 /s	7.7 /s	0.2 /s	972.4 kb/s	909.1 kb/s	55.5 kb/s	7.7 kb/s	49.1 b/s

All None Display: Sum Rate

Si personne ne se voit sur les graphes, il faut alors restart apache2 sur toutes les machines.

2) Utilisation des profils

Voici notre HTTP_TRAFFIC :



Statistics timeslot Jan 10 2020 - 17:50

Channel:	Flows:					Packets:					Traffic:				
	all:	tcp:	udp:	icmp:	other:	all:	tcp:	udp:	icmp:	other:	all:	tcp:	udp:	icmp:	other:
http	6.2 /s	1.2 /s	4.8 /s	0.2 /s	0.0 /s	218.1 /s	179.0 /s	34.0 /s	5.0 /s	0.1 /s	1.1 Mb/s	1.0 Mb/s	64.8 kb/s	5.5 kb/s	39.5 b/s
	all:	tcp:	udp:	icmp:	other:	all:	tcp:	udp:	icmp:	other:	all:	tcp:	udp:	icmp:	other:
TOTAL	6.2 /s	1.2 /s	4.8 /s	0.2 /s	0.0 /s	218.1 /s	179.0 /s	34.0 /s	5.0 /s	0.1 /s	1.1 Mb/s	1.0 Mb/s	64.8 kb/s	5.5 kb/s	39.5 b/s

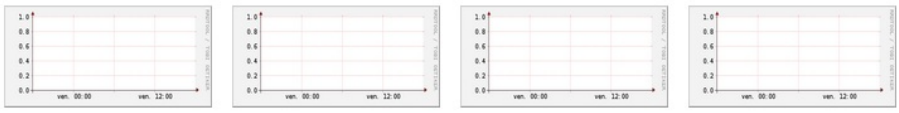
All None Display: Sum Rate

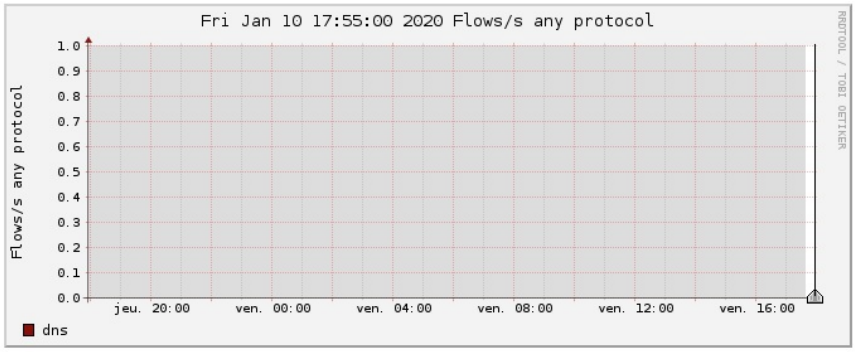
Voici notre DNS_TRAFFIC :

Home | Graphs | Details | Alerts | Stats | Plugins | continuous / shadow | Bookmark URL | Profile: dns ▼

Profile: dns

TCP **UDP** **ICMP** **other**



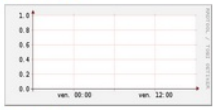


Profileinfo:

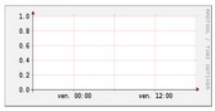
Type: continuous / shadow
Max: unlimited
Exp: never
Start: Jan 10 2020 - 17:40 CET
End: Jan 10 2020 - 17:55 CET

t_{start} 2020-01-10-17-55
t_{end} 2020-01-10-17-55

Packets



Traffic



Select [Single Timeslot] Display: [1 day] << < | ^ > >> >|

Lin Scale Stacked Graph
Log Scale Line Graph

Statistics timeslot Jan 10 2020 - 17:55

Channel:	Flows:					Packets:					Traffic:				
	all:	tcp:	udp:	icmp:	other:	all:	tcp:	udp:	icmp:	other:	all:	tcp:	udp:	icmp:	other:
dns	2.5 /s	0 /s	2.5 /s	0 /s	0 /s	2.6 /s	0 /s	2.6 /s	0 /s	0 /s	3.9 kb/s	0 b/s	3.9 kb/s	0 b/s	0 b/s
	all:	tcp:	udp:	icmp:	other:	all:	tcp:	udp:	icmp:	other:	all:	tcp:	udp:	icmp:	other:
TOTAL	2.5 /s	0 /s	2.5 /s	0 /s	0 /s	2.6 /s	0 /s	2.6 /s	0 /s	0 /s	3.9 kb/s	0 b/s	3.9 kb/s	0 b/s	0 b/s

All None **Display:** Sum Rate