R5.02: NETFLOW

Jean-Marc Pouchoulon

Septembre 2023

Ce document a pour objet d'illustrer l'analyse des flux réseaux avec Netflow.

1 Objectifs et Consignes

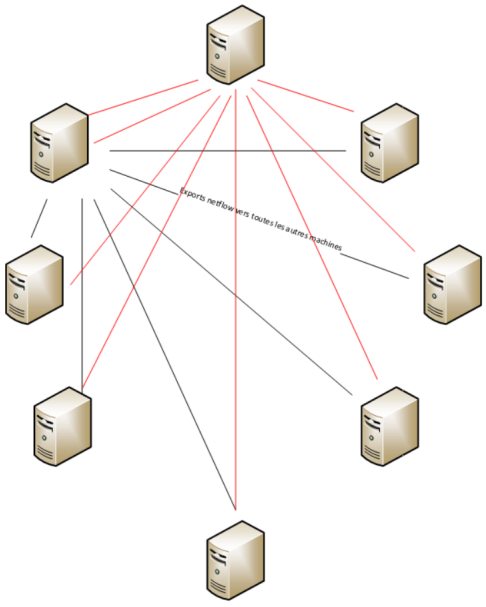
L'objectif du TP est de mettre en place de la métrologie à partir de données issues du protocole Netflow et ensuite d'analyser avec nfsen/nfdump les flux réseaux. Les livrables attendus en fin de TP sont :

- Une architecture netflow fonctionnelle et validée par l'enseignant en cours de TP (en envoi et en réception de flux).
- Un compte rendu sur le TP qui comprendra aussi les autres parties (Enisa et analyse des flux anonymisés de L'IUT via nfdump).

L'installation des sondes Netflow se fera se fera sur la VM Debian http://store.iutbeziers.fr/debianvm.ova qui sera joignable sur le réseau avec une IP indépendante de l'hôte. Vous construirez un container nfsen sur cette VM. Vous travaillez de façon individuelle mais vous devrez vous coordonner avec les autres étudiants (surtout pour le ports et IP receptionnaires des flows).

2 Réalisation d'une maquette Netflow sur la salle

Le schéma suivant montre pour deux machines que les flux Netflow partent de et à destination de chaque machine:



2.1 Configuration de la sonde fprobe

Chaque machine est donc à la fois réceptionnaire et expéditrice des flux Netflow. Au final vous serez capables de monitorer tous les flux de toutes les machines sur chacun de vos postes. L'infrastructure fonctionne sur les éléments suivants :

fprobe qui est chargée d'exporter les flux netflow vers les autres machines. L'installation de cet élément se fait classiquement par apt-get. Sa configuration se fait via le fichier /etc/default/fprobe:

```
#fprobe default configuration file

INTERFACE="eno1"
# Si vous êtes le poste 1 de la salle 213 vous exportez le flux sur toutes les Nfsen de la salle sur le port 1561
# Si vous êtes le poste 2 de la salle 213 vous exportez le flux sur toutes les Nfsen de la salle sur le port 1562
# ....

FLOW_COLLECTOR="10.213.1.2:1561 10.213.2.2:1561 10.213.3.2:1561 ..."

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

Attention seuls les ports déclarés dans le fichier docker-compose.yaml sont éligibles (1555 à 1579).

2.2 Configuration de nfsen

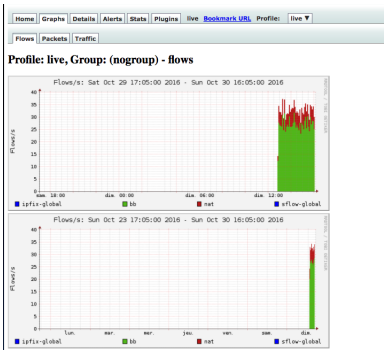
— **nfcapd** enregistre les flux envoyés par fprobe il est activé par le lancement de nfsen et **nfdump** lit les flux qui lui sont envoyés par les sondes fprobe. L'installation va se faire au travers d'un container Docker. Clonez le projet sur https://registry. iutbeziers.fr:11443/pouchou/nfsen-dockerized.git Lancer les commandes suivantes pour lancer l'application : docker-compose up -d nfsen doit être accessible sur le port 6080 de votre VM via le navigateur.

— **nfsen** qui est l'interface web de nfdump/nfcapd afin d'afficher les différents éléments remontés.

Dans le container modifiez le fichier nfsen.conf en rajoutant comme sources les autres postes de la salle et en changeant la couleur donnée sous forme hexadécimale

```
docker-compose exec nfsen bash
cd /data/nfsen/etc
   #Editez nfsen.conf  et ajoutez une ligne par poste de la salle
   'poste1'  => { 'port' => '1561', 'col' => '#50B719', 'type' => 'netflow' },
   'poste2'  => { 'port' => '1562', 'col' => '#50B719', 'type' => 'netflow' },
   ...
   # Reconfigurez nfsen:
    /data/nfsen/bin/nfsen reconfig
```

Vous deviez obtenir ce type de graphe:



3 Utilisation des profils

Générez un profil HTTP et DNS. Vous pouvez vous aider du document suivant pour le faire : `https://nsrc.org/workshops/2014/afnog-nmf/raw-attachment/wiki/Agenda/exercise4-using-NfSen-vFR.pdf` Générez du trafic http et dns et visualisez ces flux.

4 Cisco Netflow sous GNS3

Utilisez un routeur Cisco sous GNS3 et exporter ses flux via Netflow sur votre nfsen au travers d'une appliance NAT (Mettez un container afin de générer du trafic).

5 Entrainement à l'analyse de flux sur la VM de l'agence européenne de la sécurité (enisa)

Téléchargez l'image d'entrainement de l'enisa sur `http://store.iutbeziers.fr/enisaforensics.ova` et suivez le document enisa-netflow.pdf afin de vous entrainer à l'utilisation de nfsen/nfdump. Un reboot de la Vm est nécessaire.

6 Analyse des flux netflow anonymisés de l'IUT

Intégrez les statistiques depuis des fichiers anonymisés : Copiez le targz depuis l'ENT dans votre directory et détarez le dans /opt/nfsen/profiles-data/live/natiutbeziers/ via la commande "docker cp" Dans /opt/nfsen/profiles-stat/live/profile.dat remettez le status à new (status = new). Dans l'interface graphique régénérez le profile.

Reconstruisez les bases rrd via la commande :

```
/opt/nfsen/bin/nfsen -r live all
touch /opt/nfsen/profiles-stat/live/natiutbeziers.rrd
```

Pensez à remettre les droits nfsen :www-data sur l'arborescence que vous venez d'importer.

1. En utilisant l'interface graphique et après avoir sélectionné la période du 7 au 15 décembre donnez le top 10 par DST IP ordonnés par flows/packets/bytes. Quel est l'adresse la plus accédée en nombre de bytes et de "packets" ?
2. Retrouvez l'adresse responsable de l'envoi de ces flux.
3. Agrégez par srcip,srcport,dstip,dstport au format long.
4. En ligne de commande afficher les flux par protocole et trier par bytes (option -s proto/bytes ou -a -A proto) pour le mois de Décembre. A quoi correspond le protocole IGMP ?
5. En ligne de commande agrégez les flux http pour le mois de décembre.