Manipulation de la suite ELK

Elastic - Logtash – Kibana

INF726 - Sécurité

Encadrant : Julien DREANO

Laurent NGUYEN

MS Big Data Télécom Paris

15/06/2021

Table of Contents

1 Environnement....1
1.1 Machine hôte....1
1.2 Virtualisation....1
1.3 Fichiers PCAP....1
1.4 Architecture et workflow....1
2 Processus d’installation....2
2.1 Docker....2
2.2 Container Docker elk_ln....3
2.3 Parsing des flux réseaux....4
3 Visualisation....5

Index of Figures

Index of Tables

1 Environnement

1.1 Machine hôte

La machine hôte est un portable avec les caractéristiques hardware et software suivantes :

- Processeurs : Intel® Core™ i5-10210U CPU @ 1.60GHz × 8
- Mémoire RAM : 16 Go
- Disque dur : 480 Go
- Système d'exploitation : Ubuntu 20.04.2 LTS (64 bits)

1.2 Virtualisation

Pour ce projet, j'ai décidé d'utiliser une virtualisation applicative avec Docker, avec une image qui contient la suite ELK sebp/elk (https://elk-docker.readthedocs.io). Le container dispose des applications Elastic, Logstash et Kibana. Pour ce projet, je n'utiliserai pas Logtash pour l'ingestion des données, mais Packetbeat qui est spécialisé dans l'ingestion de packets réseau (comme recommandé dans le sujet du projet). L'application Packetbeat sera installée directement dans le container ELK.

Note

Au lieu d'installer l'application Packetbeat directement dans le container ELK, j'aurais pu installer Packetbeat dans un container distinct et faire communiquer les deux containers ensemble. Cette architecture serait plus adaptée au cas où les flux réseaux seraient écoutés sur une autre machine. On pourrait également dans ce cas utiliser Docker compose qui peut orchestrer plusieurs containers.

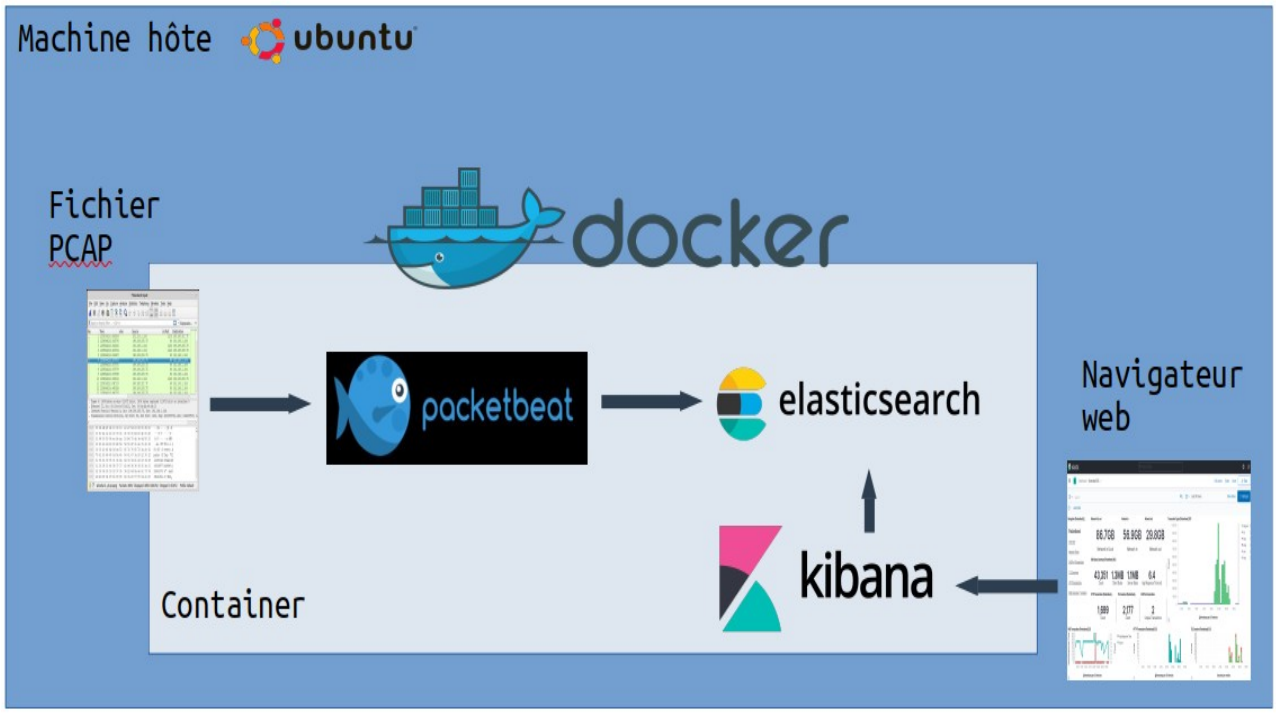
1.3 Fichiers PCAP

Les fichiers PCAP choisis sont trois fichiers résultant de la capture des flux réseaux 4SICS Geek Lounge pendant trois jours (20-21-22/10/2015). 4SICS est une conférence sur l'industrie de la cybersécurité. Le « Geek Lounge » possède un lab ICS avec des PLCs, RTUs, servers, équipements réseaux industriels (switches, firewalls, etc). Les trois fichiers ont une taille totale de 359Mo (25, 134 et 200Mo).

https://www.netresec.com/?page=PCAP4SICS

1.4 Architecture et workflow

1. Les fichiers PCAPS sont situés sur la machine hôte, sur un répertoire partagé avec le container (option –volume de Docker)
2. Packetbeat, dans le container Docker, ingère les fichiers PCAP, les transforme et les insère dans Elastic (qui est dans le même container)
3. Kibana, dont les dashboards ont été prédéfinis par Packetbeat, permet d'afficher les données dans un navigateur web sur la machine hôte


Machine hôte
ubuntu
Fichier
PCAP
docker
packetbeat
elasticsearch
Navigateur
web
kibana
Container

2 Processus d’installation

2.1 Docker

Pour installer Docker :

```
# pour s’assurer que la machine hôte est à jour
sudo apt-get update && sudo apt-get upgrade
# pour installer docker
sudo apt-get install docker
# pour augmenter les droits de l’utilisateur docker
sudo groupadd docker
sudo usermod -aG docker ${USER}
su -s ${USER}
# pour modifier les paramètres de mémoire
sysctl vm.max_map_count
sudo sysctl -w vm.max_map_count=262144
# de manière plus permanente, modifier le fichier /etc/sysctl.conf
# en ajoutant ou mettant à jour  vm.max_map_count=262144
```

Pour vérifier que docker est bien installé, on peut créer un premier container « hello-world »

```
docker run hello-world
```

2.2 Container Docker elk_ln

Pour installer la stack ELK + Packetbeat dans un container, les lignes de commande sont les suivantes :

```
# pour télécharger un container avec la stack ELK
sudo docker pull sebp/elk
# pour démarrer le container
# on précise les ports utilisés par Elastic (9200) et Kibana (5601)
# on précise la mémoire nécessaire au fonctionnement du container (4Go)
# on précise un espace d’échange entre la machine hôte et le container
# (pour utiliser les fichiers PCAP)
```

```
# on aurait également pu les télécharger directement dans le container avec wget

sudo docker run --memory="4g" -p 5601:5601 -p 9200:9200 -p 5044:5044 -v="$(pwd)/data/:/usr/data/" --name elk_ln sebp/elk

# pour entrer dans le container pour installer Packetbeat

sudo docker exec -it elk_ln /bin/bash
```

Une fois dans le container créé, on installe Packetbeat avec les commandes suivantes (pour information, on est loggué en root, donc on n'a pas besoin de préciser sudo) :

```
# pour mettre à jour le container

apt update && apt upgrade

# pour installer les applications curl, nano qui j'utiliserai plus tard

# et libpcap0.8 qui sera utiliser par Packetbeat pour ingérer les fichier PCAP

apt install curl libpcap0.8 nano

# pour télécharger et installer Packetbeat

curl -L -O https://artifacts.elastic.co/downloads/beats/packetbeat/packetbeat-7.13.0-amd64.deb

dpkg -i packetbeat-7.13.0-amd64.deb
```

Ensuite, on met à jour le fichier de configuration de Packetbeat :

```
nano /etc/packetbeat/packetbeat.yml
```

Dans la partie Kibana, on met à jour 2 lignes :

```
setup.dashboards.enabled: true

host: "localhost:5601"
```

Ensuite, on teste la configuration de Packetbeat :

```
# pour tester le fichier de configuration

packetbeat test config

# pour tester l'output

packetbeat test output

# pour configurer les dashboard Kibana par défaut de Packetbeat

packetbeat setup

# si on veut lancer Packetbeat pour écouter les flux réseaux
```

```
service packetbeat start

service packetbeat enable
```

Dans notre cas, nous allons ingérer 3 fichiers PCAP

```
packetbeat -I /usr/data/4SICS-GeekLounge-151020.pcap && packetbeat -I
/usr/data/4SICS-GeekLounge-151021.pcap && packetbeat -I /usr/data/4SICS-
GeekLounge-151022.pcap
```

Note

Les packets ingérés avec un fichier PCAP ne gardent pas leur timestamp original mais le timestamp de lecture du fichier.

Pour ingérer des fichiers plus rapidement, on peut utiliser l'option -t, pas ex : packetbeat -t -I /usr/data/4SICS-GeekLounge-151020.pcap

2.3 Parsing des flux réseaux

La configuration par défaut de Packetbeat est utlisée pour parser les flux réseaux. Elle permet de lire notamment les adresses IP sources et destination, le nombre et la taille des paquets réseaux ainsi que les protocoles utilisés. Elle permet également d'avoir des informations plus spécifiques à certains protocoles réseaux et flux de bases de données (ICMP (v4 and v6), DHCP (v4), DNS, HTTP, AMQP 0.9.1, Cassandra, Mysql, PostgreSQL, Redis, Thrift-RPC, MongoDB, Memcache, NFS, TLS, SIP/SDP (beta)).

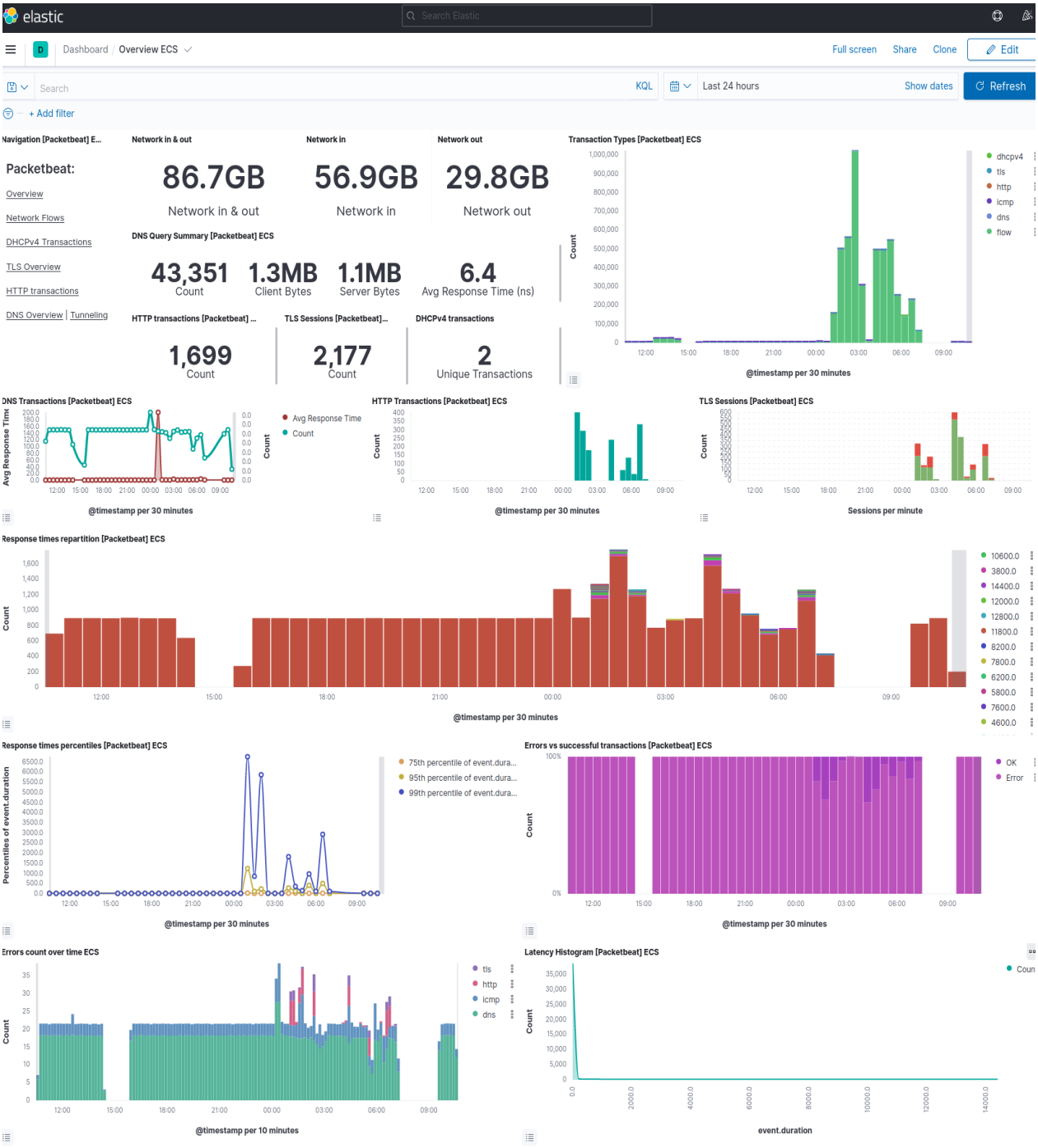
3 Visualisation

Kibana est utilisé pour visualiser les données. L'application se présente sous la forme d'une page web accessible à l'url suivante : http://localhost:5601

En installant Packetbeat, j'ai exporté les dashboards Packetbeat par défaut dans Kibana (commande : packetbeat setup). Ces dashboards sont complets et présentent déjà une bonne première version. J'ai adapté ces dashboards à notre cas d'usage (les fichiers PCAPS de 4SICS 2015). Les principales modifications sont :

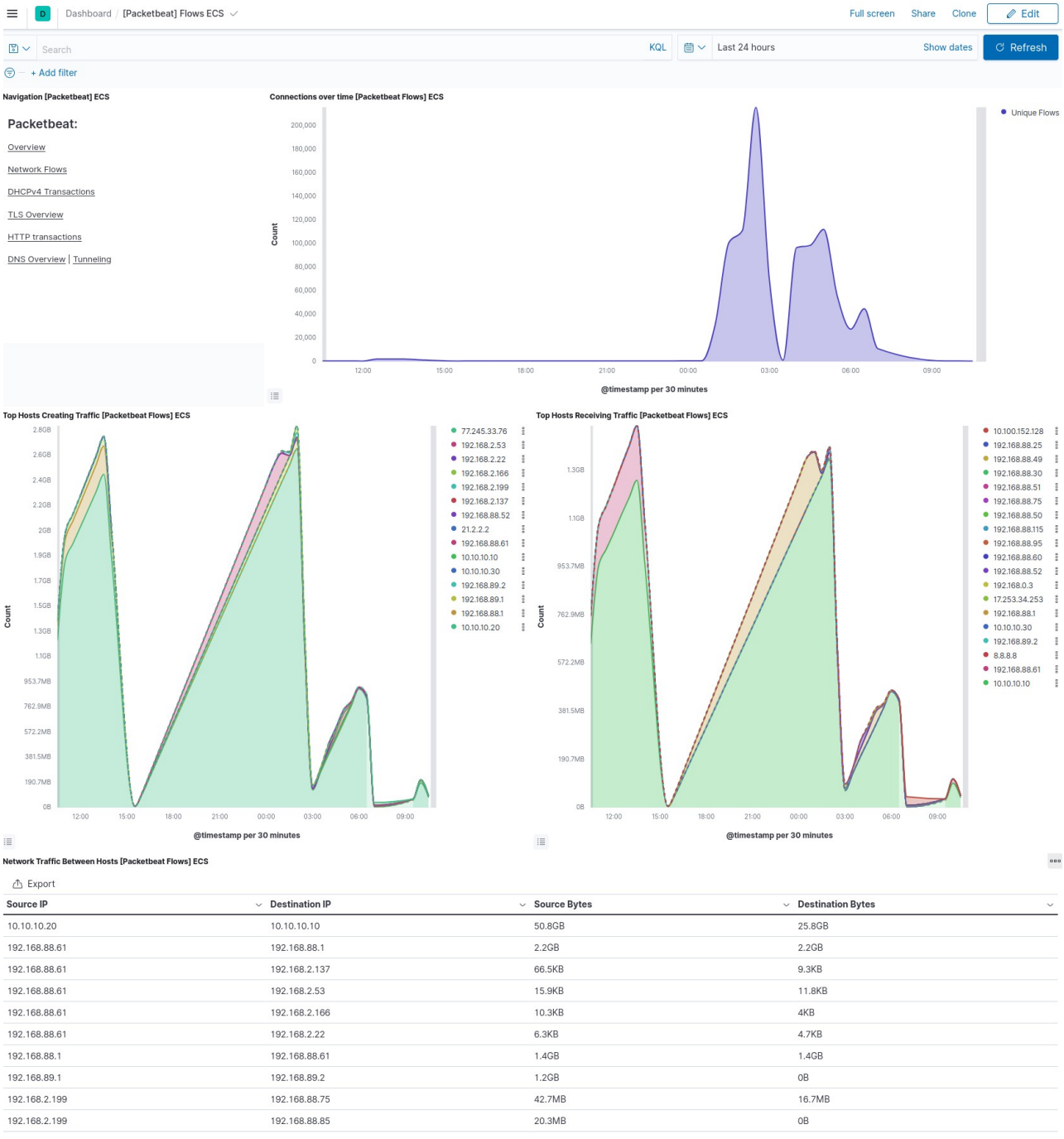
- Dashboard Overview :
  - la carte de localisation des adresses source et destination est remplacée car les fichiers PCAP portent sur des flux d'un réseau local ; il n'est donc pas pertinent de géolocaliser les « machines »
  - pour avoir une vue globale des flux réseaux ont été ajoutés quelques indicateurs / widgets (dont certains créés à partir de Kibana Discover) :
    - Taille des flux réseaux in & out, in puis out
    - Nombre de transactions DNS, HTTP, sessions TLS et transactions uniques DHCPv4
  - Ont été gardés : l'évolution des types de transactions, des transactions DNS, HTTP, sessions TLS, répartition des temps de réponse et taux d'erreur, latence
- Suppression des dashboards spécifiques aux bases de données car il n'y avait pas de tels flux

○


elastic
Search Elastic
Dashboard / Overview ECS
Full screen
Share
Clone
Edit
Search
KQL
Last 24 hours
Show dates
Refresh
+ Add filter
Navigation [Packetbeat] E...
Packetbeat:
Overview
Network Flows
DHCPv4 Transactions
TLS Overview
HTTP transactions
DNS Overview | Tunneling
Network in & out
86.7GB
Network in & out
Network in
56.9GB
Network in
Network out
29.8GB
Network out
DNS Query Summary [Packetbeat] ECS
43,351
Count
1.3MB
Client Bytes
1.1MB
Server Bytes
6.4
Avg Response Time (ns)
HTTP transactions [Packetbeat] ...
1,699
Count
TLS Sessions [Packetbeat]...
2,177
Count
DHCPv4 transactions
2
Unique Transactions
Transaction Types [Packetbeat] ECS
dhcpv4
tls
http
icmp
dns
flow
Count
@timestamp per 30 minutes
DNS Transactions [Packetbeat] ECS
Avg Response Time
Count
@timestamp per 30 minutes
HTTP Transactions [Packetbeat] ECS
@timestamp per 30 minutes
TLS Sessions [Packetbeat] ECS
Sessions per minute
Response times repartition [Packetbeat] ECS
@timestamp per 30 minutes
Response times percentiles [Packetbeat] ECS
75th percentile of event.dura...
95th percentile of event.dura...
99th percentile of event.dura...
Percentiles of event.duration
@timestamp per 30 minutes
Errors vs successful transactions [Packetbeat] ECS
OK
Error
@timestamp per 30 minutes
Errors count over time ECS
tls
http
icmp
dns
@timestamp per 10 minutes
Latency Histogram [Packetbeat] ECS
event.duration

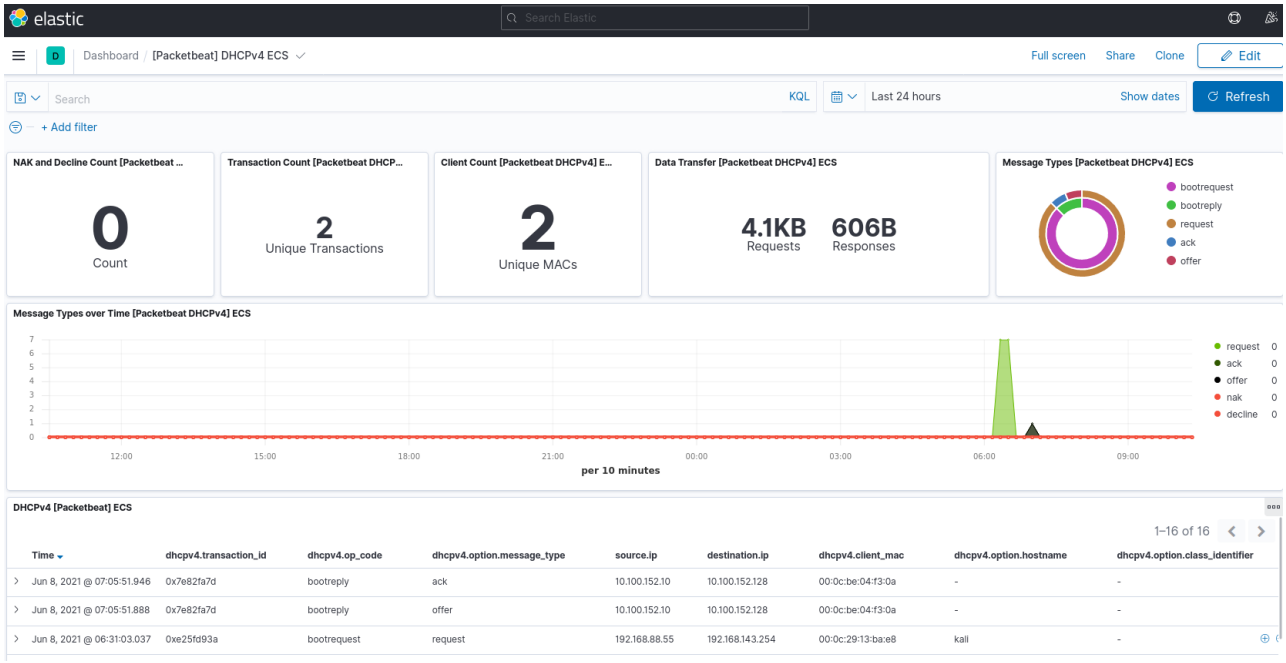
Les autres dashboards ont été conservés :

- Dashboard Network flows : évolution du nombre de connexions, les « tops hosts » créant et recevant du traffic

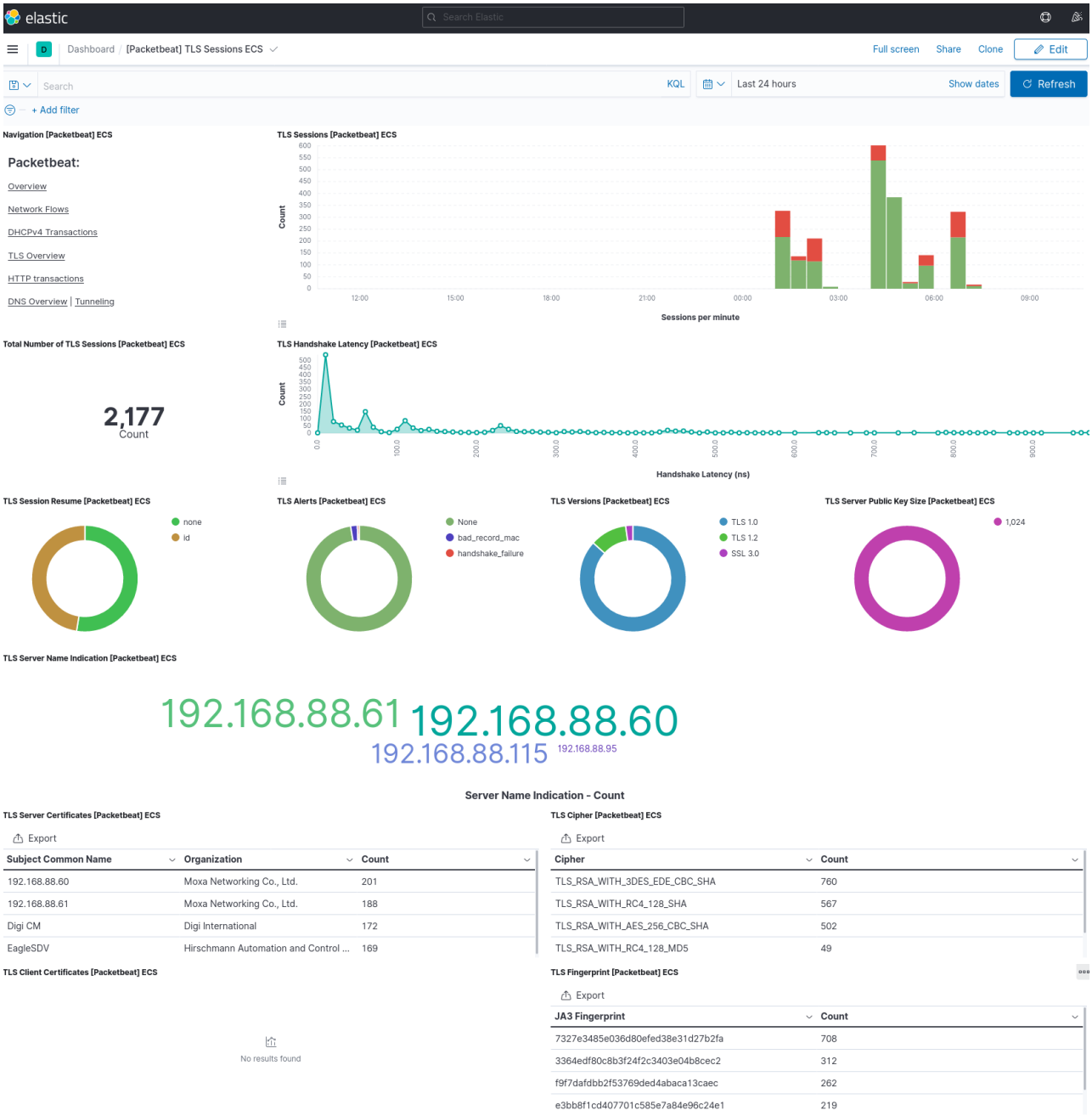


Source IP	Destination IP	Source Bytes	Destination Bytes
10.10.10.20	10.10.10.10	50.8GB	25.8GB
192.168.88.61	192.168.88.1	2.2GB	2.2GB
192.168.88.61	192.168.2.137	66.5KB	9.3KB
192.168.88.61	192.168.2.53	15.9KB	11.8KB
192.168.88.61	192.168.2.166	10.3KB	4KB
192.168.88.61	192.168.2.22	6.3KB	4.7KB
192.168.88.1	192.168.88.61	1.4GB	1.4GB
192.168.89.1	192.168.89.2	1.2GB	0B
192.168.2.199	192.168.88.75	42.7MB	16.7MB
192.168.2.199	192.168.88.85	20.3MB	0B

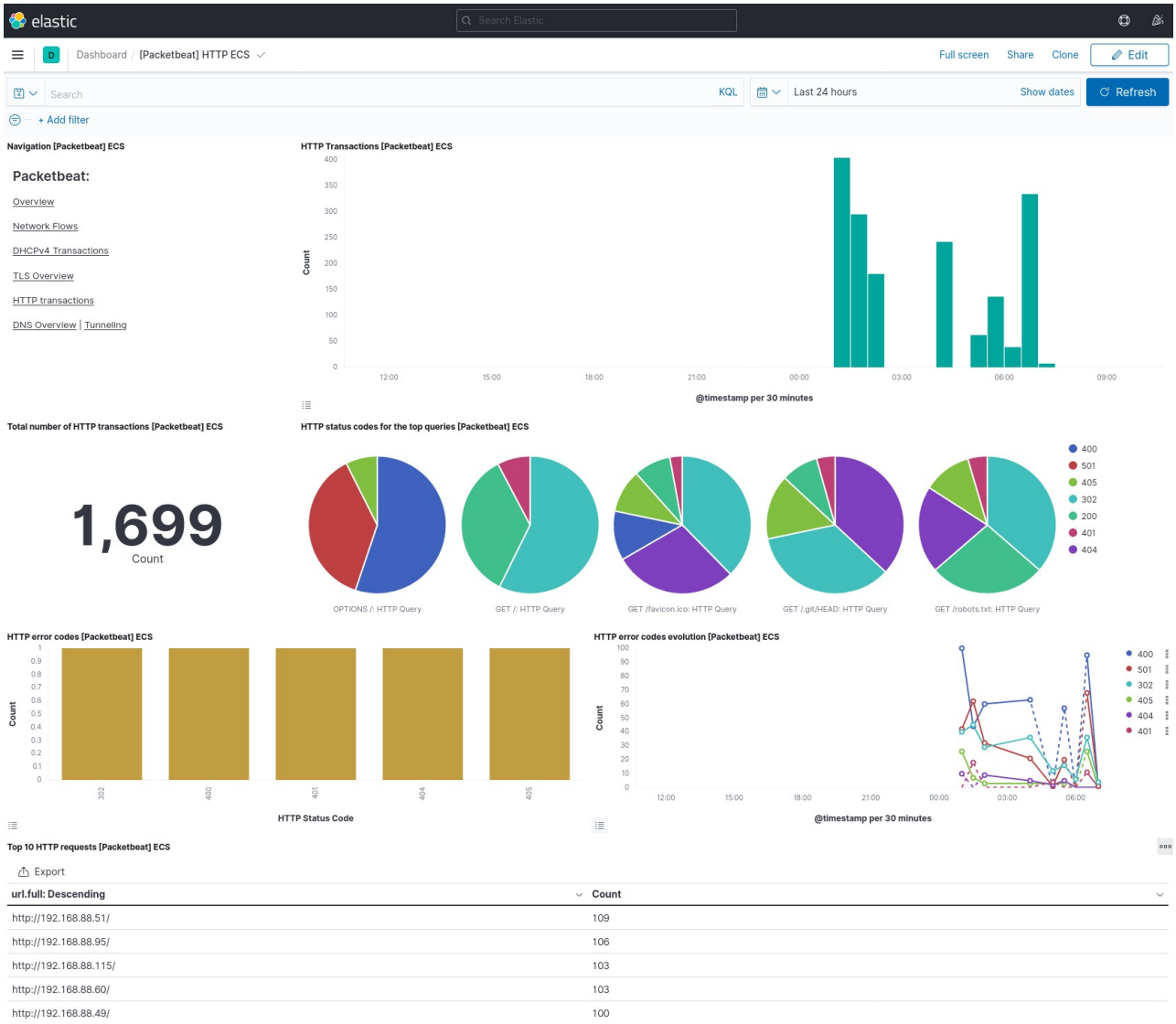
- Dashboard DHCPv4 transactions :



- Dashboard TLS Overview : évolutions des sessions TLS, erreurs TLS, versions TLS



- Dashboard HTTP transactions : évolutions des transactions HTTP, proportions des codes réponses HTTP



Top 10 HTTP requests [Packetbeat] ECS

Export

url.full: Descending	Count
http://192.168.88.51/	109
http://192.168.88.95/	106
http://192.168.88.115/	103
http://192.168.88.60/	103
http://192.168.88.49/	100

- Dashboard DNS Overview / Tunneling : chiffres clefs et évolution des requêtes DNS, tunneling DNS