VagrantとAnsibleを用いたフロー情報の可視化環境作成

富士通株式会社

梅野　崇

2019/07/24

はじめに

※発表内容は発表者個人によるものであり、会場や組織を代表するものではありません。

- Wiresharkで大量のパケット(1GB以上)を追うのは大変
- ネットワークのフロー情報から有用な情報を得たい
- netflowやIPfixのフロー情報の可視化環境構築は面倒

↓

- VagrantとAnsibleで下記のフロー情報の可視化環境を構築
  - YAF,nDPI,super_mediatorでフロー情報抽出
  - ElasticStack,Grafanaでフロー情報の可視化

- メモリ8GB以上のWindows, Mac, Linuxで動作
- visualize network traffic by ELK6
  - https://github.com/t-umeno/visualize_network_traffic
  - https://github.com/t-umeno/visualize_network_traffic/blob/master/README.ja.md
  - https://www.slideshare.net/TakashiUmeno/visualizenetworktraffic-20181108-122136601

VagrantとAnsibleで生成するVMの構成

- NICから受信したパケットをYAF(nDPI使用)でIPfix形式のフロー情報に変換
- IPfixをsuper_mediatorでJSONファイルに変換
- JSONファイルをLogstash経由でElasticsearchに入力
- Elasticsearchでフロー情報検索
- Webブラウザで下記表示
  - KibanaでElasticsearchの検索結果
  - Grafanaでフロー数、オクテット数、パケット数

動作環境

- メモリ8GB以上のWindows,Mac,Linux
- 対象となるネットワークに接続可能なNIC
- git
- VirtualBox
- Vagrant
- vagrant-disksize plugin
- vagrant-proxyconf plugin (http proxy使用環境)
- vagrant-vbguest (オプション)
- firefox or chrome (IE, edge不可)

インストール

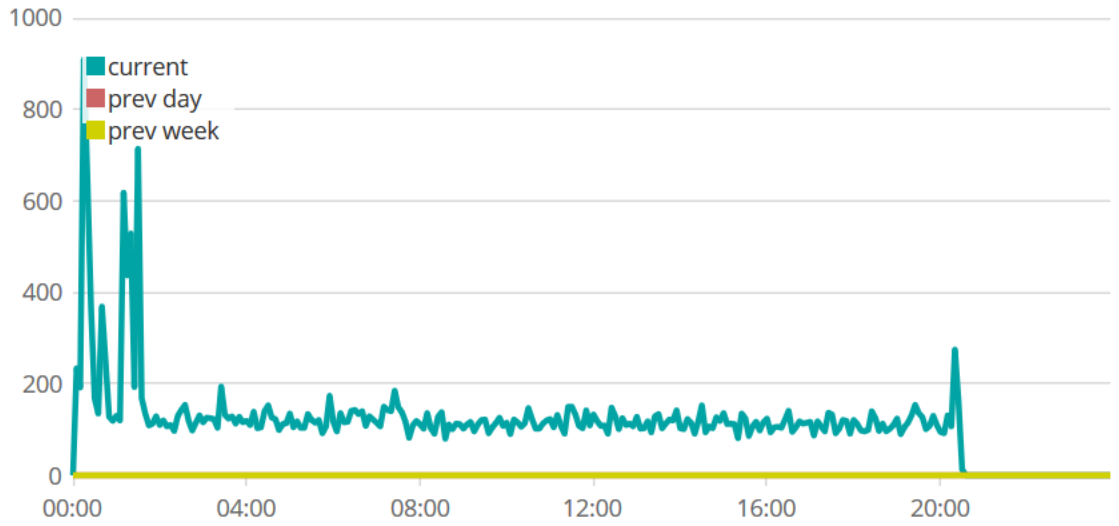
```
$ export http_proxy="http://aaa.bbb.ccc.ddd:8080/" # option
$ export https_proxy="http://aaa.bbb.ccc.ddd:8080/" # option
$ vagrant plugin install vagrant-proxyconf # if you use proxy
$ vagrant plugin install vagrant-vbguest # option
$ vagrant plugin install vagrant-disksize
$ cd ansible/ELK6/playbooks
$ vagrant up
(snip)
(select network interface for packet capture)
==> default: Available bridged network interfaces:
1) en1: Wi-Fi (AirPort)
2) bridge0
3) en0: Ethernet
4) en2: Thunderbolt 1
5) p2p0
==> default: When choosing an interface, it is usually the one that is
==> default: being used to connect to the internet.
 default: Which interface should the network bridge to? 3
```

ダッシュボード表示

- Kibana
  - フロー数推移(当日、1日前、1週間前)
  - DNS
    - 問い合わせ名, IPアドレスなど
  - オクテット数推移
  - フロー数(IP,Port,MAC,TCPフラグ,プロトコル番号で分類)
  - http
    - Referer, Get, UserAgent, ServerStringなど
  - SSL
  - nDPIによるアプリケーション解析
    - (Google, Office365, Twitterなど)
  - SYNにSYN+ACKを返さないホスト(ユニークな相手ホスト数TOP10)
  - オクテット数が多いTOP10
- Grafana
  - フロー数
  - オクテット数(順方向、逆方向)
  - パケット数(順方向、逆方向)
  - フロー数、オクテット数、パケット数でアラートを送信する際に使用
  - メールやslackなどGrafanaで使用可能な手段でアラートを通知可能

Add a filter +

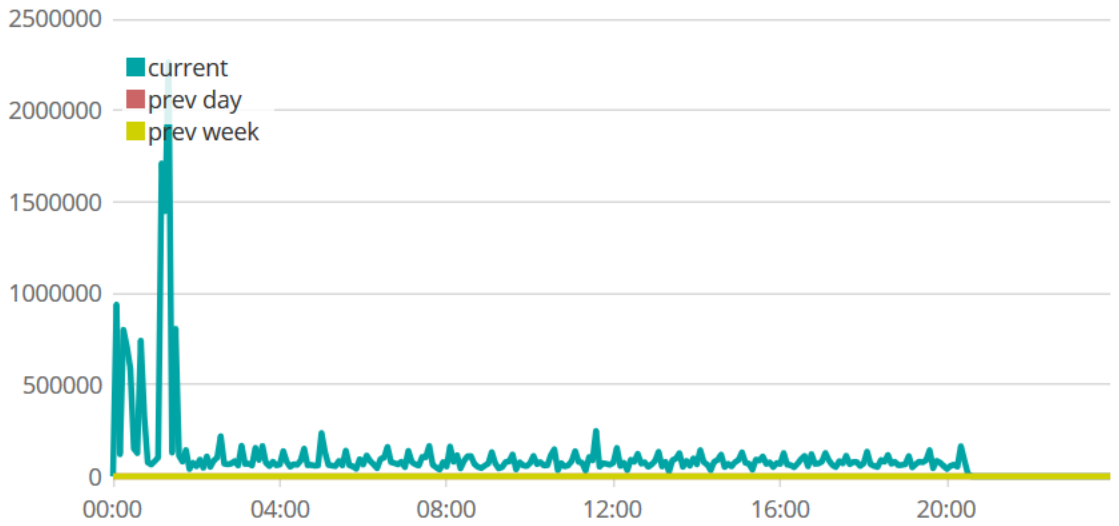
flows count current prev day prev week



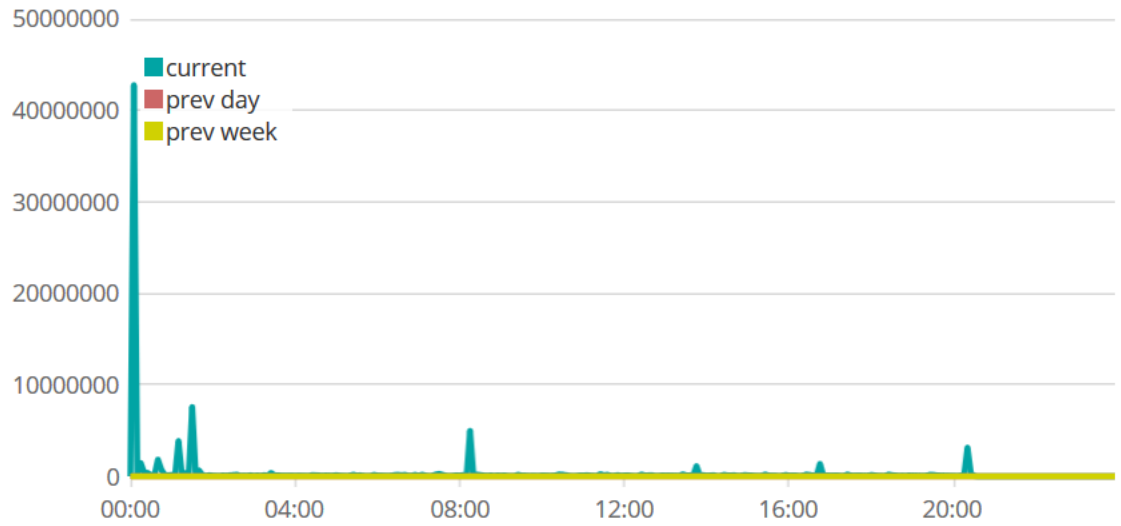
flows.dnsRecord.dnsQName

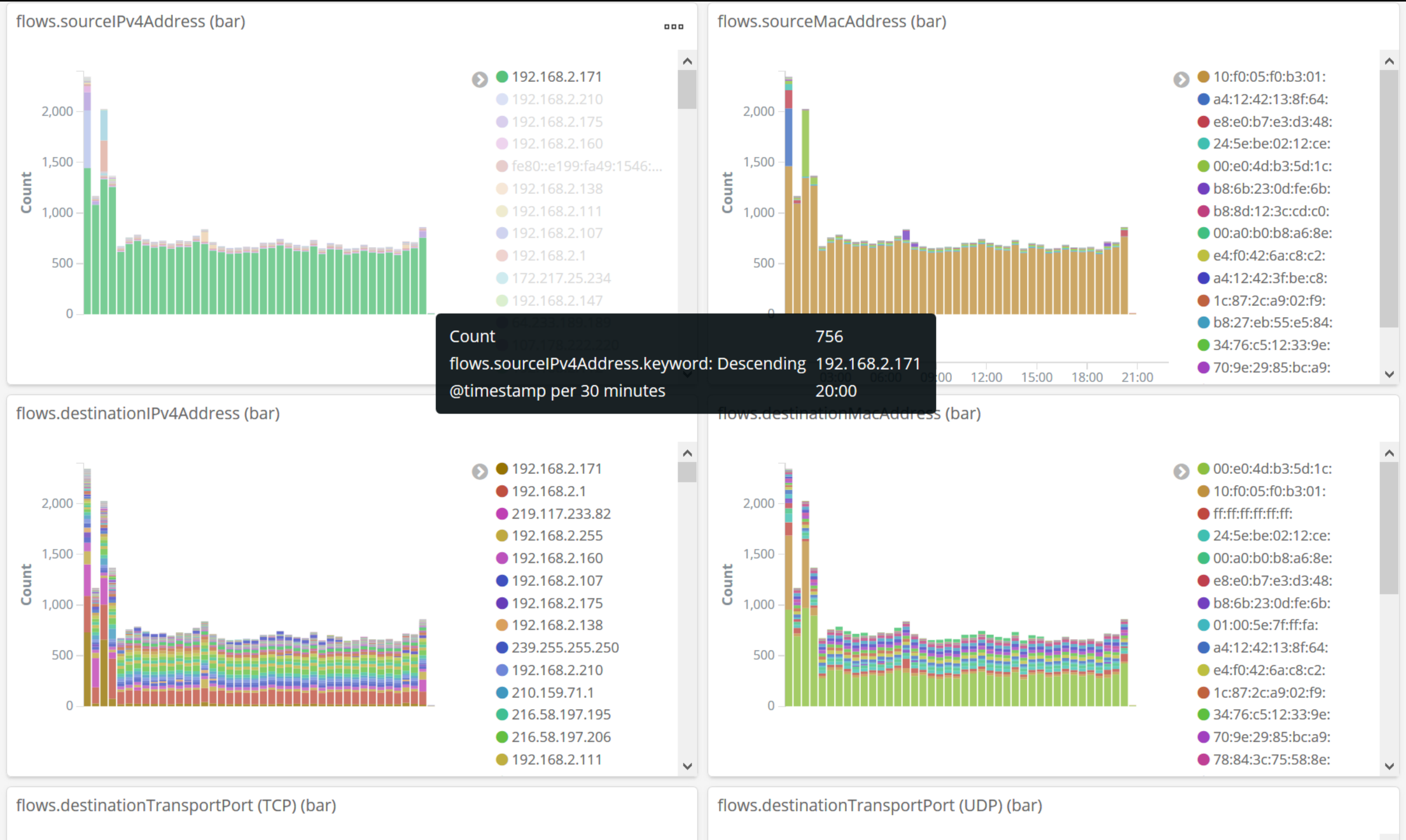
flows.dnsRecord.dnsQName.keyword: Descending	Count
news.l.google.com.	395
grafana.com.	369
raw.githubusercontent.com.	366
clients.l.google.com.	352
play.google.com.	316
plus.l.google.com.	313
fastly.net.	244
ws12.gti.mcafee.com.	225

flows.octetTotalCount current prev day prev week

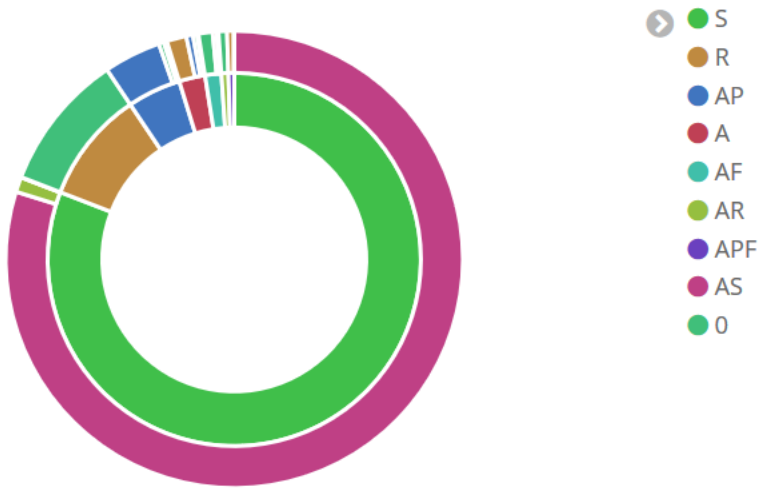


flows.reverseOctetTotalCount current prev day prev week

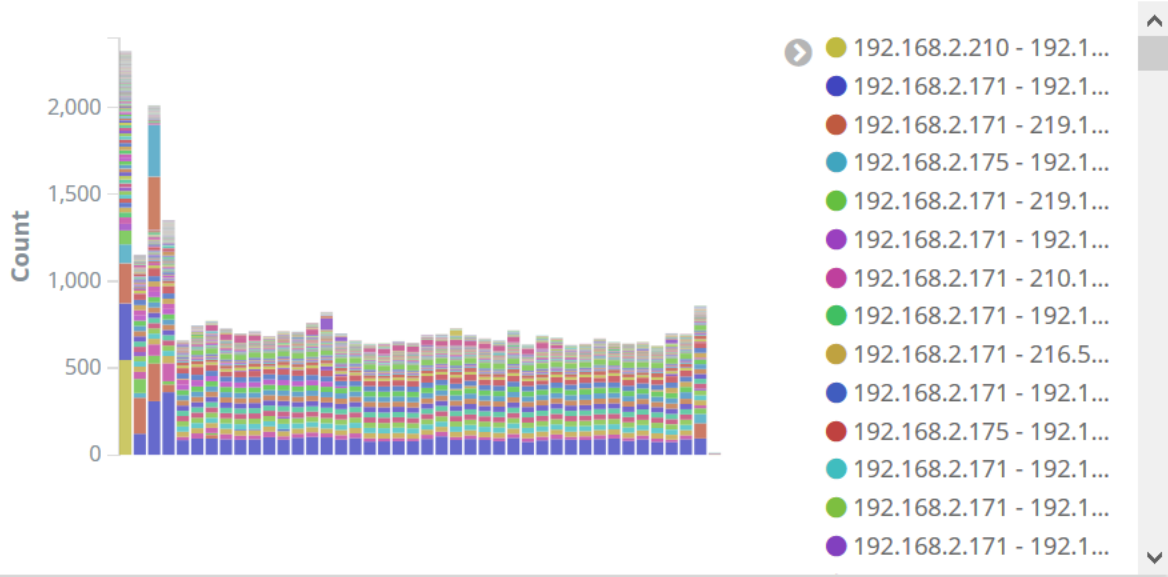



flows.sourceIPv4Address (bar)
Count
2,000
1,500
1,000
500
0
192.168.2.171
192.168.2.210
192.168.2.175
192.168.2.160
fe80::e199:fa49:1546:...
192.168.2.138
192.168.2.111
192.168.2.107
192.168.2.1
172.217.25.234
192.168.2.147
Count 756
flows.sourceIPv4Address.keyword: Descending 192.168.2.171
@timestamp per 30 minutes 20:00
flows.sourceMacAddress (bar)
12:00
15:00
18:00
21:00
10:f0:05:f0:b3:01:
a4:12:42:13:8f:64:
e8:e0:b7:e3:d3:48:
24:5e:be:02:12:ce:
00:e0:4d:b3:5d:1c:
b8:6b:23:0d:fe:6b:
b8:8d:12:3c:cd:c0:
00:a0:b0:b8:a6:8e:
e4:f0:42:6a:c8:c2:
a4:12:42:3f:be:c8:
1c:87:2c:a9:02:f9:
b8:27:eb:55:e5:84:
34:76:c5:12:33:9e:
70:9e:29:85:bc:a9:
flows.destinationIPv4Address (bar)
192.168.2.171
192.168.2.1
219.117.233.82
192.168.2.255
192.168.2.160
192.168.2.107
192.168.2.175
192.168.2.138
239.255.255.250
192.168.2.210
210.159.71.1
216.58.197.195
216.58.197.206
192.168.2.111
flows.destinationMacAddress (bar)
00:e0:4d:b3:5d:1c:
10:f0:05:f0:b3:01:
ff:ff:ff:ff:ff:ff:
24:5e:be:02:12:ce:
00:a0:b0:b8:a6:8e:
e8:e0:b7:e3:d3:48:
b8:6b:23:0d:fe:6b:
01:00:5e:7f:ff:fa:
a4:12:42:13:8f:64:
e4:f0:42:6a:c8:c2:
1c:87:2c:a9:02:f9:
34:76:c5:12:33:9e:
70:9e:29:85:bc:a9:
78:84:3c:75:58:8e:
flows.destinationTransportPort (TCP) (bar)
flows.destinationTransportPort (UDP) (bar)

flows.TCPFlags



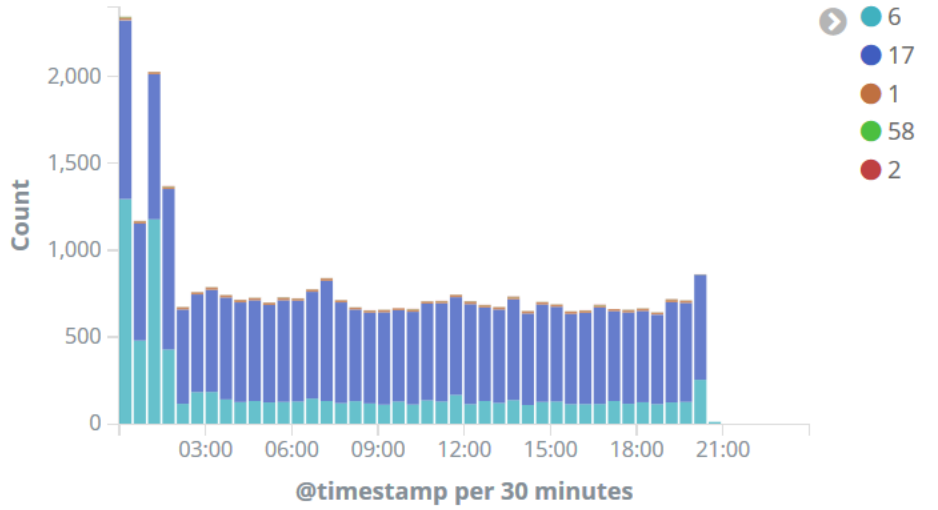
src_ip_dst_ip_port_proto (bar)



flows.httpHost

flows.httpHost.keyword: Descending	Count
belldandy.v4.unnumbered.net	268
content.dellsupportcenter.com	124
scrootca2.ocsp.secomtrust.net	40
192.168.2.160:8200	37
go.microsoft.com	31
192.168.2.107:55247	29
192.168.2.175:20001	21
scrootca1.ocsp.secomtrust.net	20

flows.protocolIdentifier (bar)



flows.httpReferer

flows.httpGet

@timestamp per 30 minutes

flows.httpReferer

flows.httpReferer.keyword: Descending	Count
http://news.livedoor.com/article/detail/15651482/	27
http://news.livedoor.com/css/v2/common.css?v=2.58	5
https://news.google.com/	1

flows.httpGet

flows.httpGet.keyword: Descending
GET /mstr/pd.txt?pr=Vostro%205471&os=Win%2010%20%2817134.407%29&build=6. id=b9f1ba87-08db-48f8-b9f4-05067ba2c09d&dl=true&saaver=3.0.2.48&wr=2022%2F
GET /mstr/pd.txt?pr=Vostro%205471&os=Win%2010%20%2817134.407%29&build=6. id=b9f1ba87-08db-48f8-b9f4-05067ba2c09d
GET /MEowSDBGMEQwQjAJBgUrDgMCGgUABBTyDvPjcY8Z0TDZzHotwwMWHLKc0AQUCo %3D%3D
GET /

flows.httpUserAgent.keyword

flows.httpUserAgent.keyword: Descending	Count
Microsoft-WebDAV-MiniRedir/10.0.17134	268
aws-sdk-cpp/1.2.9 Windows/10.0.17134.376 AMD64	123
Microsoft-CryptoAPI/10.0	69
Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:63.0) Gecko/20100101 Firefox/63.0	54
Microsoft-Windows/10.0 UPnP/1.0	52
User-Agent: Microsoft-DLNA DLNADOC/1.50	40
Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML	37

flows.httpServerString

flows.httpServerString.keyword: Descending	Count
Apache/2.4.37	270
3.4.6-generic Microsoft-Windows/6.1 Windows-Media-Player-DMS/12.0.7601.17514 DLNADOC/1.50 UPnP/1.0	37
Linux/2.x.x, UPnP/1.0, pvConnect UPnP SDK/1.0, Twonky UPnP	17
ECS	14
Unspecified, UPnP/1.0,	7
Apache/2.4.18	5
unspecified, UPnP/1.0	4

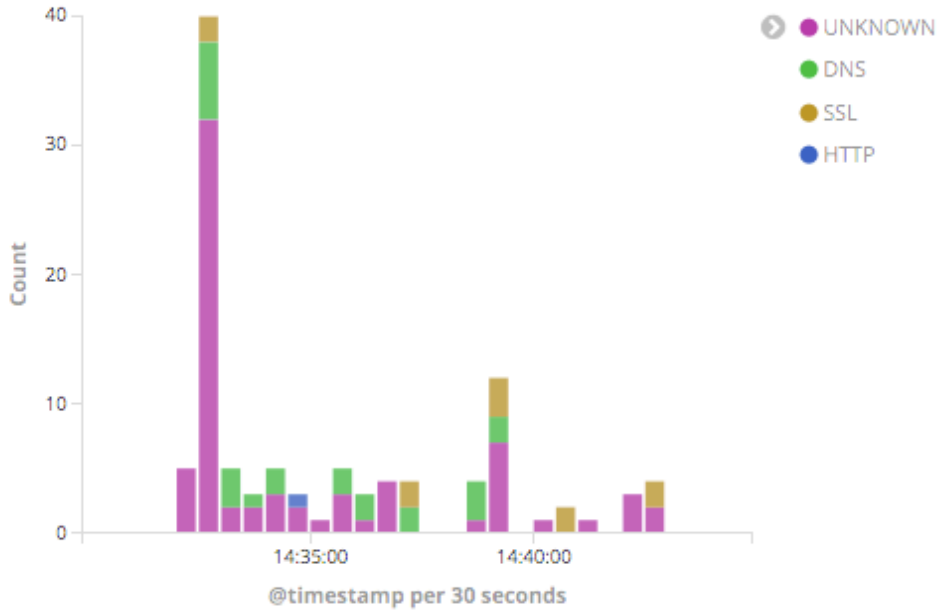
kibana

- Discover
- Visualize
- Dashboard
- Timelion
- Canvas
- Maps
- Machine Learning
- Infrastructure
- Logs
- APM
- Uptime
- Dev Tools
- Monitoring
- Management

D Default

Collapse

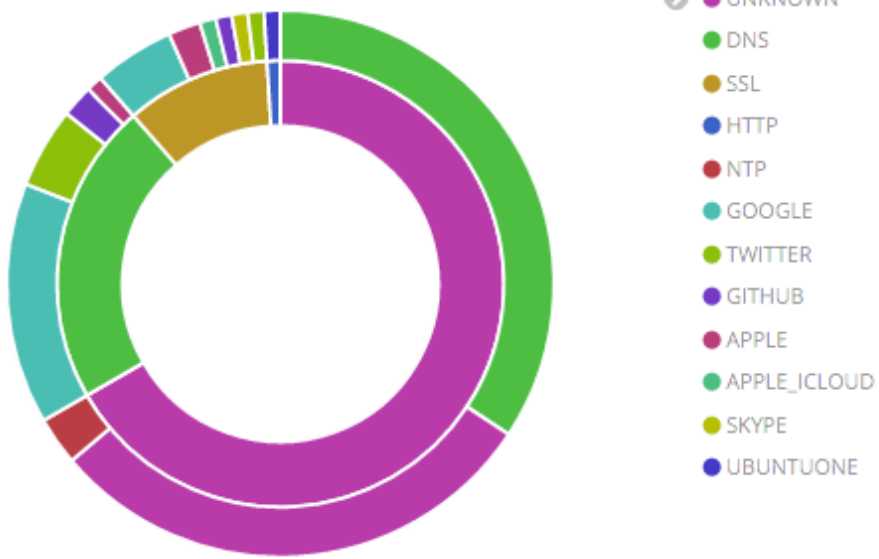
nDPIL7Protocol_str(bar)



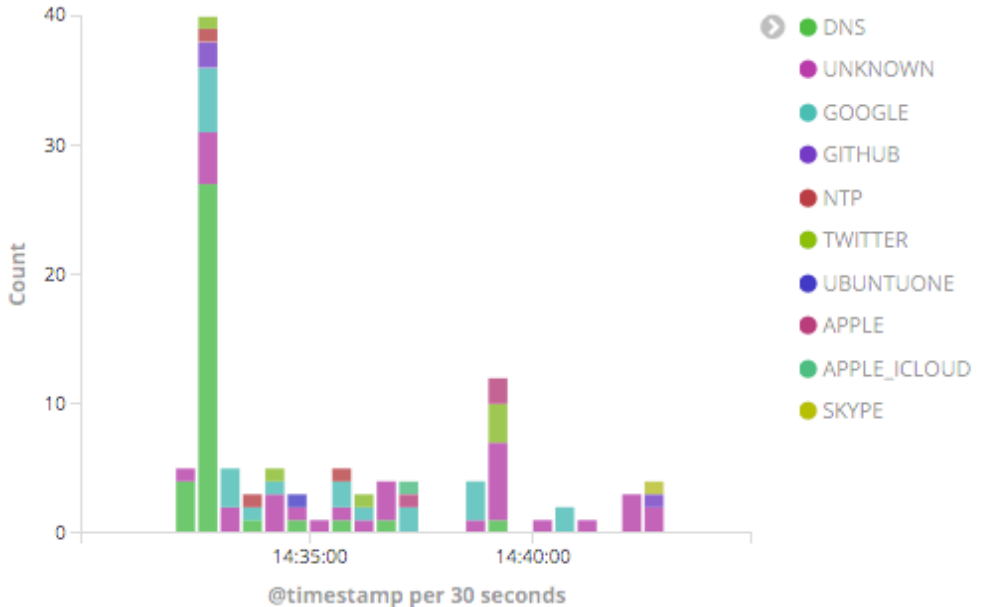
flows.httpServerString

No results found

nDPI

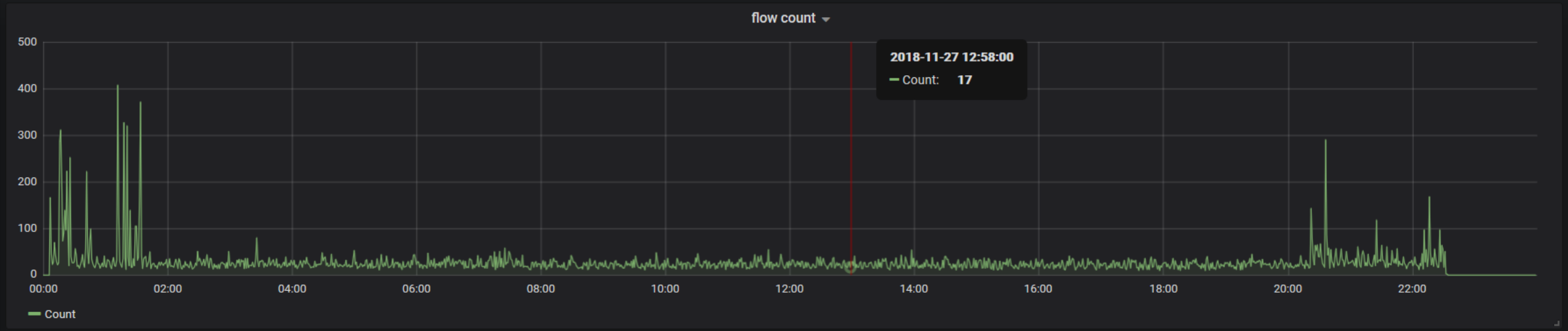


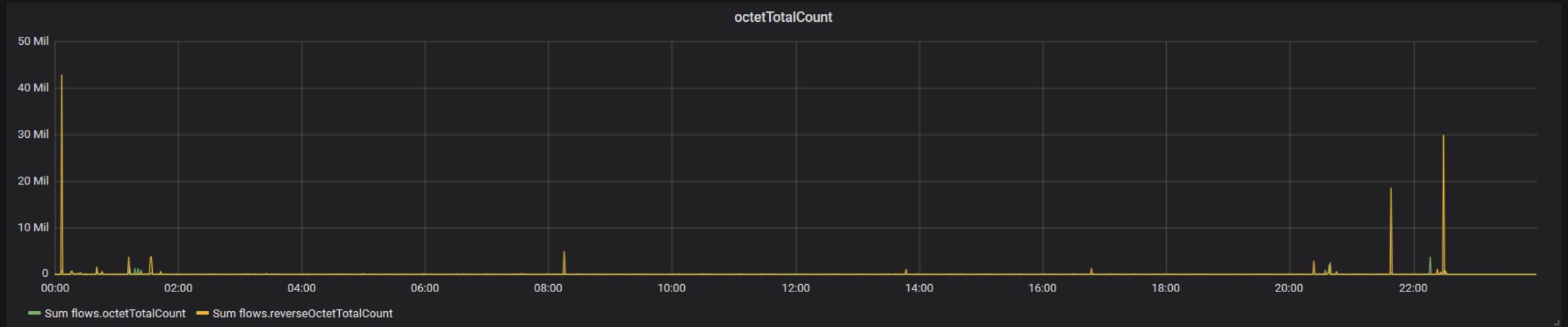
nDPIL7SubProtocol_str (bar)

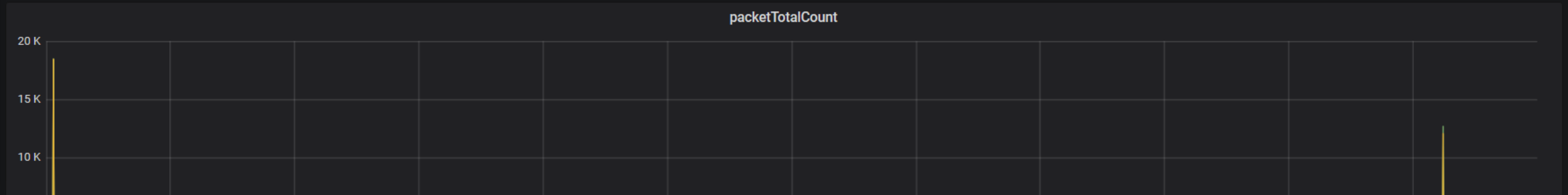


ElasticSearch YAF count

Today Refresh every 1m







ご清聴ありがとうございました