`elastiflow`: *netflows* en ELK

Iñigo Ortiz de Urbina Cazenave
AS64512

Introducción

- `$(whoami)`
  - Iñigo Ortiz de Urbina Cazenave
  - Miembro de la comunidad con ganas de compartir
- **No** es mi software

Introducción

- `$(whoami)`
  - Iñigo Ortiz de Urbina Cazenave
  - Miembro de la comunidad con ganas de compartir
- **No** es mi software
  - Ni lo uso en producción 🤗

elastiflow: ¿qué es?

- Sistema de colección y visualización de flujos de red basado en ELK
  - **E**lasticsearch: almacenamiento y consulta
  - **L**ogstash: recepción, decodificación, *encaminamiento*
  - **K**ibana: tableros de mandos, informes

elastiflow: ¿qué es?

- Alternativa a `nfsen(-ng)`, `nfcapd`, etc
  - Ecosistema inactivo
    - Comunidad, soporte y desarrollo limitados
- Alternativa a opciones propietarias
  - Ecosistema inactivo
    - Comunidad, soporte y desarrollo limitados
    - Y además, habitualmente de pago 😂

elastiflow: ¿por qué me gusta?

- Libre
- `netflow v5/v9, sFlow, ipfix`
- Basado en ELK
  - Horizontalmente escalable*
  - Personalizable extensible
  - Diagnostico *basado en ELK*

elastiflow: ¿por qué me gusta?

- Plug and play
- Configuración por defecto *sensata*
- Índices
  - Identificadores de aplicaciones (Fortinet, Cisco)
  - Identificacores de protocolo
  - Identificadores de servicio
  - *Flags* TCP

elastiflow: valoración

- Ventajas
  - Basado en infra de propósito general
  - U[IX] moderna
  - Extensible
  - Escalable
  - Diagnosticable
  - Despliegue sencillo
  - Datos normalizados y enriquecidos
- Desventajas
  - Basado en infra de propósito general
    - Rendimiento
  - Dependencias significativas
  - Precisión
    - No apto para facturación

La *no* demo 🤡

- Configuración de *andar por casa*
  - Gateway (PC Engines APU)
    - OpenBSD configurado con OpenHRC™
    - `set state-defaults pflow`
  - Server (Mac Mini 2011)
    - Ubuntu 18.04 LTS
    - ELK + elastiflow *a mano*

La *no* demo 🤡

- Perspectiva general
- Top-N
- Amenazas
- Flujos
- Geo IP

- Tráfico entre ASs
- Exportadores
- Tráfico detallado
- Registro de flujos

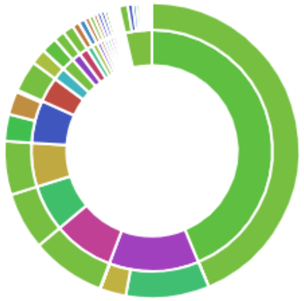
Flow Exporter: 10.0.0.1

Client: Select...

Server: Select...

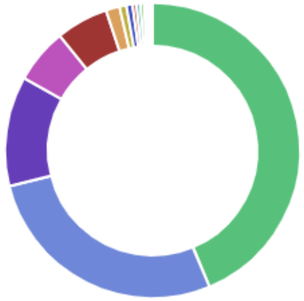
Service: Select...

Servers and Clients (bytes)



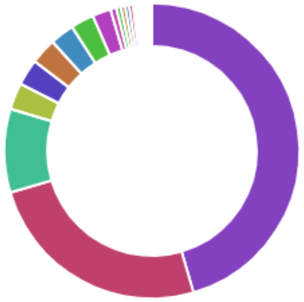
- 170-182-144-85.ftt...
- 10.0.0.12
- ipv4_1.cxl0.c114.a...
- ipv4_1.cxl0.c092.a...
- ipv4_1.mce0.c147....
- 10.0.0.6
- ipv4_1.cxl0.c057.a...
- nlams2-vip-bx-001...
- 10.0.0.52
- 88.red-81-45-105.s...
- 76.red-81-45-105.s...

Services (bytes)



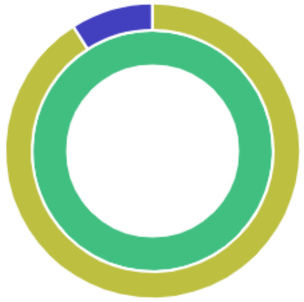
- TCP/15836
- https (TCP/443)
- plex (TCP/32400)
- http (TCP/80)
- UDP/51413
- https (UDP/443)
- asmps (TCP/45001)
- rs-status (TCP/450...
- UDP/14205
- UDP/23569
- dns (UDP/53)

Autonomous Systems (bytes)

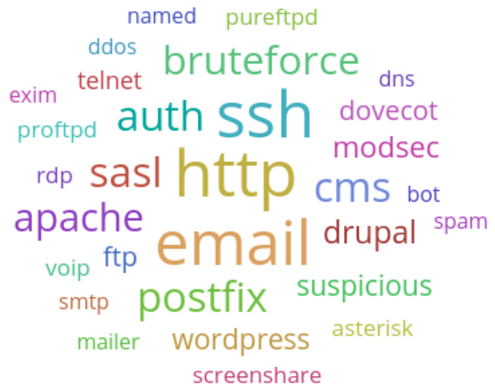


- T-Mobile Thuis BV ...
- Netflix Streaming ...
- KPN B.V. (1136)
- Netorn LLC (34123)
- Euskaltel S.A. (123...
- Apple Inc. (6185)
- Telefonica De Espa...
- Saudi Telecom Co...
- Google LLC (15169)
- Facebook, Inc. (32...
- Fastly (54113)

IP Versions and Protocols (bytes)



- IPv4
- TCP
- UDP
- ICMP
- IGMP



event.type: "ipfix" | node.hostname: "10.0.0.1" | Add a filter + | Actions

Overview | Top-N | **Threats** | **Flows** | **Geo IP** | **AS Traffic** | **Exporters** | **Traffic Details** | **Flow Records**

Talkers | **Services** | **Conversations** | **Apps**

ElastiFlow

Flow Type

ipfix

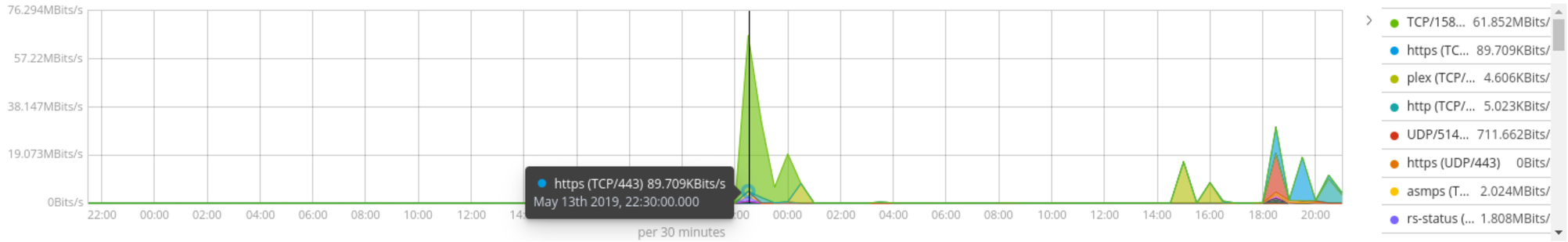
Flow Exporter

10.0.0.1

Service

Select...

Services (bits/s)



Top Clients	Bytes	Packets	Flow Records
10.0.0.52	42.741GB	33,988,000	15,796
ip503ca186.speed.planet.nl	5.404GB	4,400,170	164
host185-94-172-162.stknet.ru	1.73GB	1,826,298	12
50.85-85-82.dynamic.clientes.euskaltel.es	1.692GB	1,275,208	28
95.218.131.30	1.503GB	1,596,222	12
10.0.0.60	1.365GB	1,250,754	4,847
10.0.0.55	1.135GB	1,256,776	6,224
170-182-144-85.ftth.glasoperator.nl	1.028GB	823,978	228
10.0.0.9	889.558MB	871,186	6,356
10.0.0.6	859.383MB	1,327,420	68,084
	59.18GB	**51,692,719**	**1,673,089**

Export: Raw Formatted

1 2 3 4 5 ... 50 »

Top Servers	Bytes	Packets	Flow Records
170-182-144-85.ftth.glasoperator.nl	25.869GB	20,112,722	628
10.0.0.12	7.127GB	5,907,246	1,300
ipv4_1.cxl0.c114.ams001.ix.nflxvideo.net	4.818GB	3,883,310	36
ipv4_1.cxl0.c092.ams001.ix.nflxvideo.net	3.706GB	2,990,904	36
ipv4_1.mce0.c147.ams001.ix.nflxvideo.net	3.474GB	2,825,054	112
10.0.0.6	3.386GB	3,767,559	91,416
ipv4_1.cxl0.c057.ams001.ix.nflxvideo.net	2.006GB	1,616,340	16
nlams2-vip-bx-001.aaplimg.com	1.021GB	857,258	88
10.0.0.52	1.009GB	789,370	294
88.red-81-45-105.staticip.rima-tde.net	726.382MB	593,058	36
	59.18GB	**51,690,868**	**1,672,758**

Export: Raw Formatted

1 2 3 4 5 ... 50 »

kibana

Flow Type

ipfix

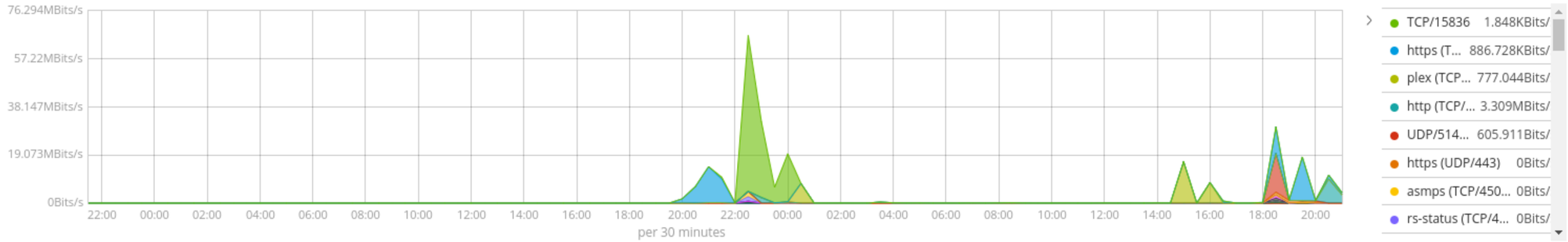
Flow Exporter

10.0.0.1

Service

Select...

Services (bits/s)



Top Services	Bytes	Packets	Flow Records
TCP/15836	25.869GB	20,112,722	628
https (TCP/443)	16.33GB	14,090,700	39,154
plex (TCP/32400)	7.129GB	5,918,808	1,860
http (TCP/80)	3.552GB	3,220,414	8,188
UDP/51413	3.377GB	3,641,928	9,278
https (UDP/443)	910.106MB	805,274	1,824
asmps (TCP/45001)	455.485MB	348,104	4
rs-status (TCP/45002)	406.714MB	310,570	8
UDP/14205	262.179MB	270,888	12
UDP/23569	260.859MB	273,196	16
	59.281GB	**51,834,988**	**1,682,656**

Export: Raw Formatted

Top IP Protocols	Bytes	Packets	Flow Records
TCP	53.934GB	44,411,920	165,919
UDP	5.332GB	7,204,997	1,476,223
ICMP	14.828MB	218,512	40,800
IGMP	56B	2	2
	59.281GB	**51,835,431**	**1,682,944**

Export: Raw Formatted

event.type: "ipfix" | node.hostname: "10.0.0.1" | Add a filter + | Actions

Overview | Top-N | **Threats** | **Flows** | **Geo IP** | **AS Traffic** | **Exporters** | **Traffic Details** | **Flow Records**

Talkers | **Services** | Conversations | **Apps**

ElastiFlow

Flow Type

ipfix

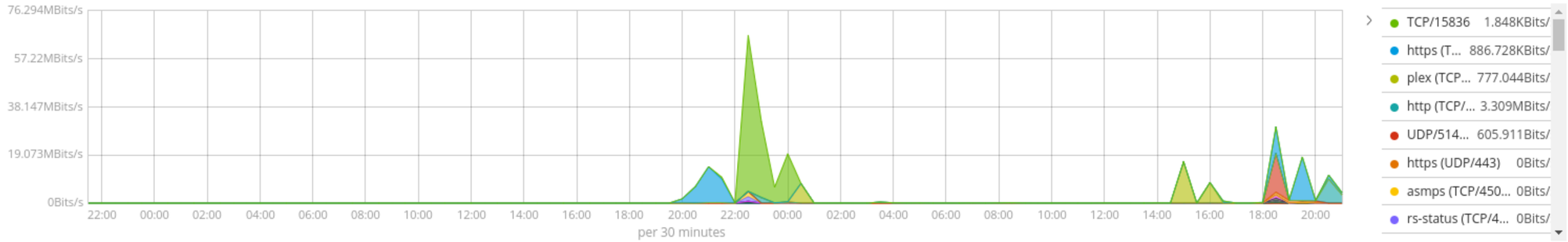
Flow Exporter

10.0.0.1

Service

Select...

Services (bits/s)



Client	Server	Service	Bytes	Packets	Flow Records
10.0.0.52	170-182-144-85.ftth.glasoperator.nl	TCP/15836	25.866GB	20,107,008	432
ip503ca186.speed.planet.nl	10.0.0.12	plex (TCP/32400)	5.404GB	4,400,170	164
10.0.0.52	ipv4_1.cxl0.c114.ams001.ix.nflxvideo.net	https (TCP/443)	4.818GB	3,883,310	36
10.0.0.52	ipv4_1.cxl0.c092.ams001.ix.nflxvideo.net	https (TCP/443)	3.706GB	2,990,904	36
10.0.0.52	ipv4_1.mce0.c147.ams001.ix.nflxvideo.net	https (TCP/443)	3.474GB	2,825,054	112
10.0.0.52	ipv4_1.cxl0.c057.ams001.ix.nflxvideo.net	https (TCP/443)	2.006GB	1,616,340	16
host185-94-172-162.stknet.ru	10.0.0.6	UDP/51413	1.73GB	1,826,298	12
50.85-85-82.dynamic.clientes.euskaltel.es	10.0.0.12	plex (TCP/32400)	1.692GB	1,275,208	28
95.218.131.30	10.0.0.6	UDP/51413	1.503GB	1,596,202	8
10.0.0.60	nlams2-vip-bx-001.aaplimg.com	http (TCP/80)	1.021GB	856,082	8
			58.818GB	**49,965,908**	**644,651**

Export: Raw Formatted

kibana

event.type: "ipfix" | node.hostname: "10.0.0.1" | Application | Add a filter + | Actions

Overview | Top-N | Threats | Flows | Geo IP | AS Traffic | Exporters | Traffic Details | Flow Records

Talkers | Services | Conversations | Apps

ElastiFlow

Flow Type

ipfix

Flow Exporter

10.0.0.1

Application

Select...

Applications (bits/s)

No data to display for the selected metrics

No results found

No results found

kibana

Flow Type

ipfix

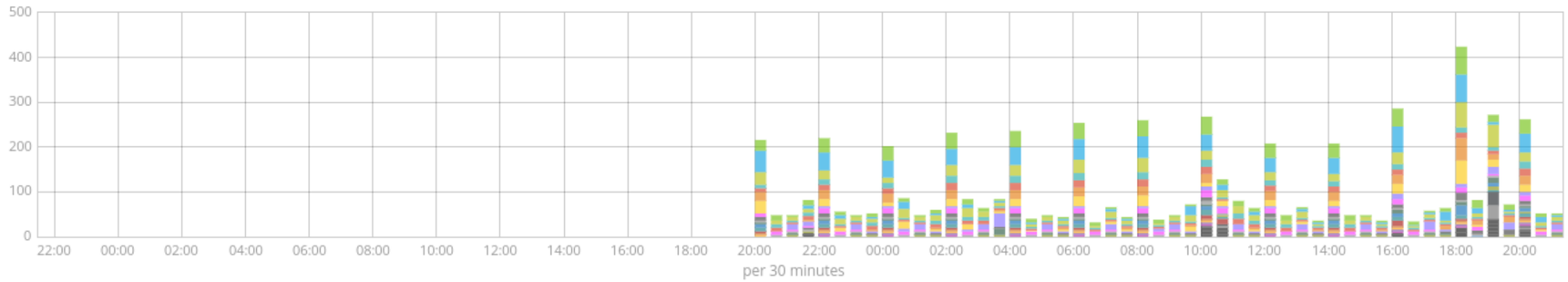
Flow Exporter

10.0.0.1

Service

Select...

IP Reputations (flows)



IP Reputations	Flows
http	764
ssh	754
email	720
auth	380
sasl	380
cms	376
postfix	370
bruteforce	350
apache	320
drupal	180

Export: Raw Formatted

1 2 3 4 »

Public Threats	IP Address	Flows
184.75.221.179	184.75.221.179	104
ip-13-60-52-196.melbourne.au.asianpacifictelephone.com	196.52.60.13	104
ip-69-60-52-196.melbourne.au.asianpacifictelephone.com	196.52.60.69	104
185.107.45.41	185.107.45.41	76
e82-103-140-214s.easyspeedy.dk	82.103.140.214	76
163.251.187.194.in-addr.arpa	194.187.251.163	64
115.251.187.194.in-addr.arpa	194.187.251.115	52
133.227.232.109.in-addr.arpa	109.232.227.133	52
149.162.152.213.in-addr.arpa	213.152.162.149	52
15.107.202.109.in-addr.arpa	109.202.107.15	52

Export: Raw Formatted

1 2 3 4 5 »

At-Risk Servers	IP Address	Flows
10.0.0.6	10.0.0.6	213

Export: Raw Formatted

High-Risk Clients	IP Address	Flows
dhcp-077-249-216-006.chello.nl	77.249.216.6	332
10.0.0.6	10.0.0.6	288
10.0.0.5	10.0.0.5	4

Export: Raw Formatted

event.type: "ipfix" | node.hostname: "10.0.0.1" | Add a filter + | Actions

Overview | **Top-N** | **Threats** | **Flows** | **Geo IP** | **AS Traffic** | **Exporters** | **Traffic Details** | **Flow Records**

Client/Server | **Src/Dst** | **AS**

ElastiFlow

Flow Exporter: 10.0.0.1

Client: Select...

Server: Select...

Service: Select...

Clients (flow records)

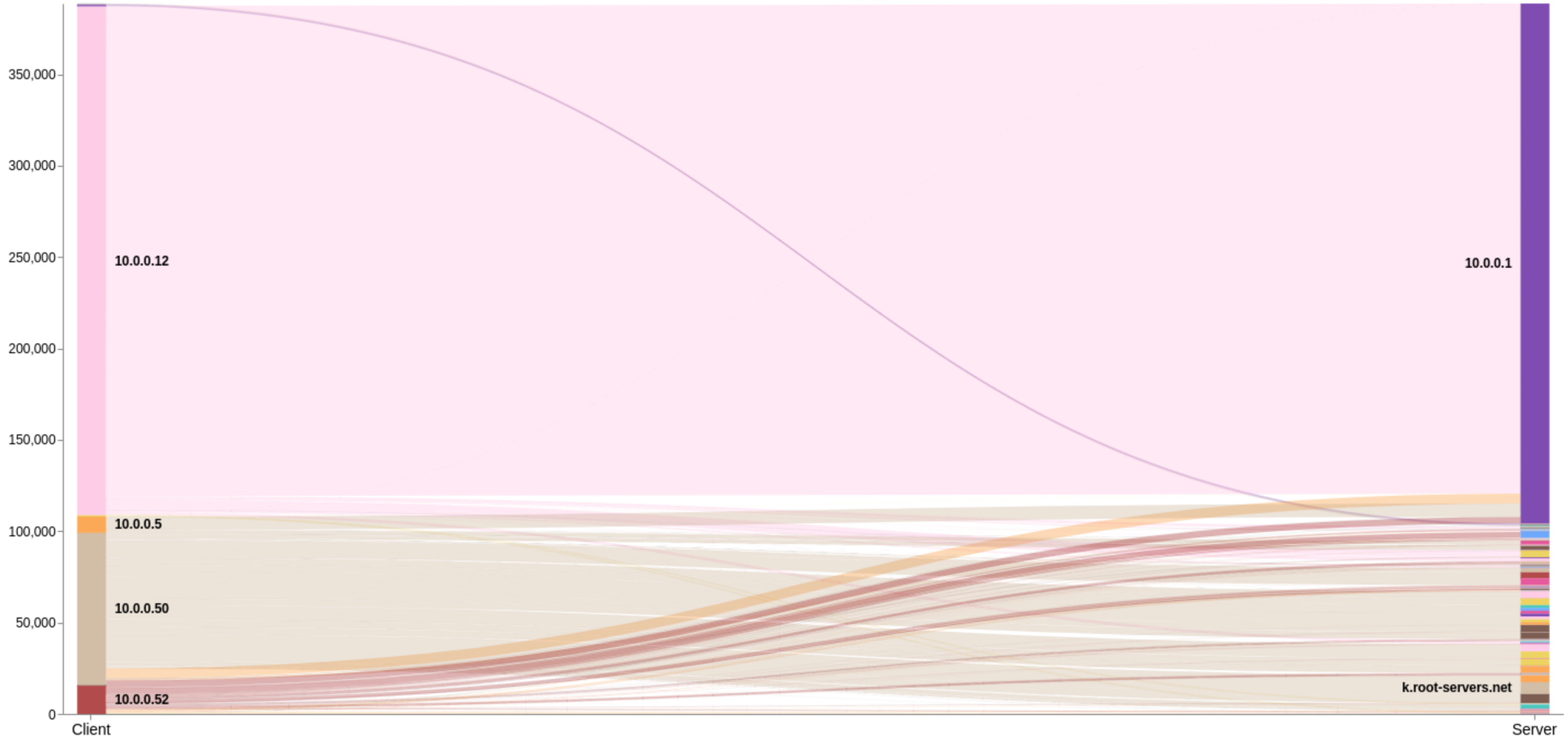
- dhcp-077-249-216-...
- 10.0.0.12
- 10.0.0.50
- 10.0.0.6
- 10.0.0.52
- 10.0.0.5

Servers (flow records)

- 10.0.0.1
- 10.0.0.6
- ns2.surfnet.nl
- ns1.surfnet.nl
- ns1.zurich.surf.net
- ns3.surfnet.nl

Services (flow records)

- dns (UDP/53)
- ICMP/8
- https (TCP/443)
- ssdp (UDP/1900)
- UDP/51413
- http (TCP/80)



kibana

event.type: "ipfix" | node.hostname: "10.0.0.1" | NOT Source AS Private | NOT Destination AS Private | Add a filter + | Actions

Overview | **Top-N** | **Threats** | **Flows** | **Geo IP** | **AS Traffic** | **Exporters** | **Traffic Details** | **Flow Records**

Client/Server | **Src/Dst** | **AS**

ElastiFlow

Flow Exporter: 10.0.0.1

Source AS: Select...

Destnation AS: Select...

Service: Select...

Source AS (flow records)

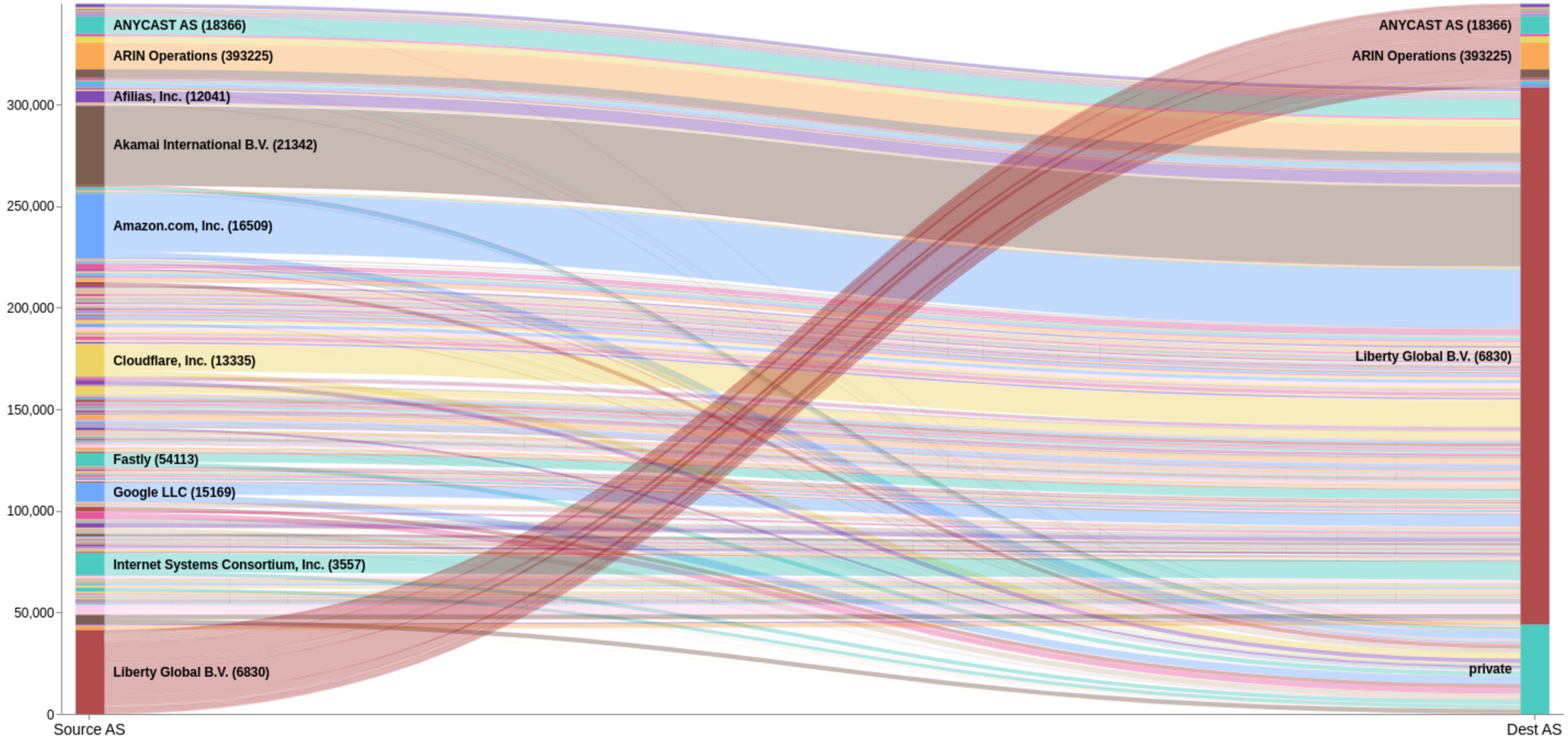
- Liberty Global B.V. ...
- Akamai Internatio...
- Amazon.com, Inc. (...
- SURFnet bv (1103)
- Reseaux IP Europe...
- WoodyNet (42)

Destination AS (flow records)

- Liberty Global B.V. ...
- Akamai Internatio...
- Amazon.com, Inc. (...
- SURFnet bv (1103)
- Cloudflare, Inc. (13...
- Reseaux IP Europe...

Services (flow records)

- dns (UDP/53)
- ICMP/8
- https (TCP/443)
- ssdp (UDP/1900)
- UDP/51413
- http (TCP/80)



kibana

event.type: "ipfix" | node.hostname: "10.0.0.1" | flow.dst_autonomous_system: "Reseaux IP Europeens Network Coordination Centre (RIPE NCC) (197000)" | Add a filter ✚ | Actions

Overview | **Top-N** | **Threats** | **Flows** | **Geo IP** | **AS Traffic** | **Exporters** | **Traffic Details** | **Flow Records**

Client/Server | **Src/Dst** | **AS**

ElastiFlow

Flow Exporter: 10.0.0.1

Source: Select...

Destnation: Select...

Destination Port: Select...

Sources (flow records)

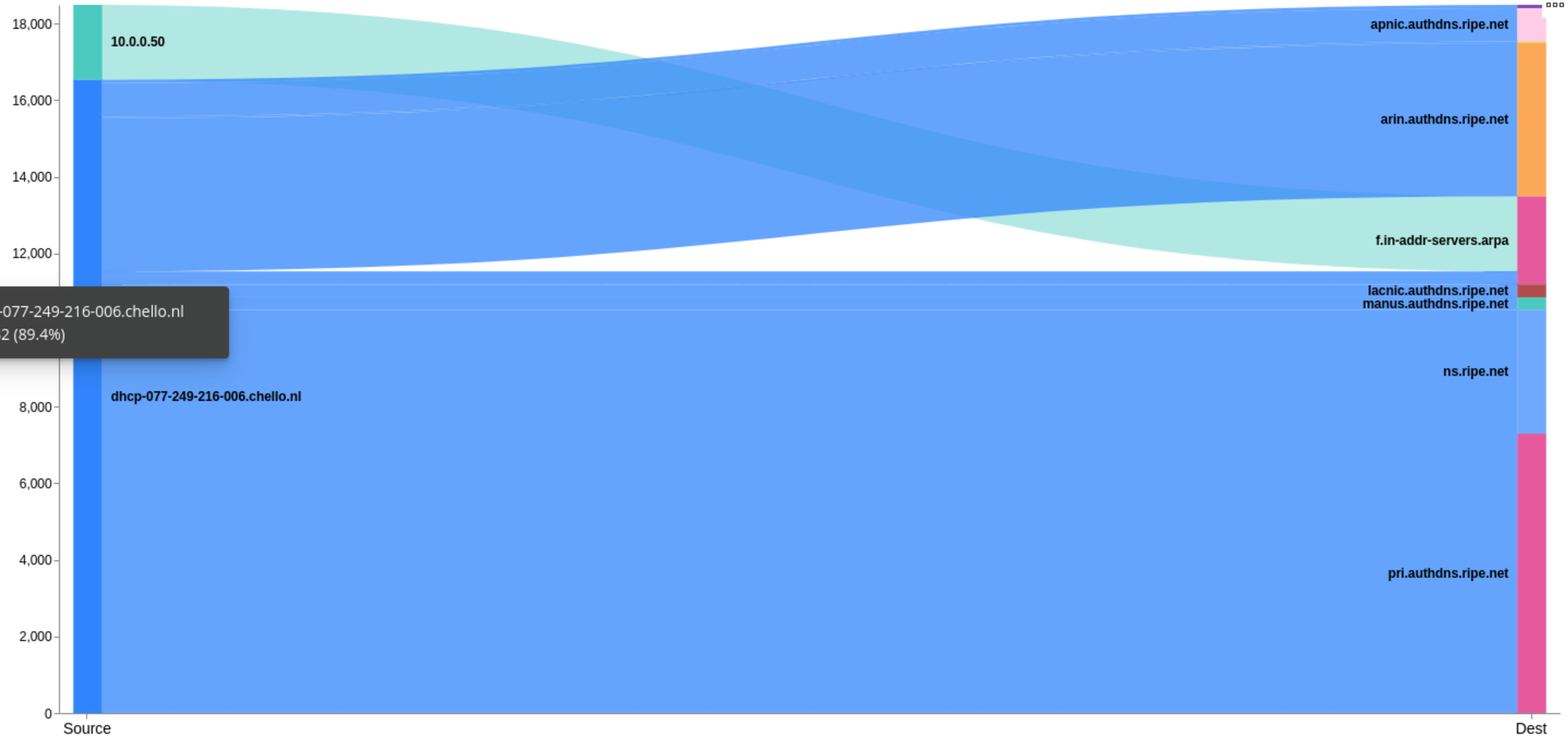
- dhcp-077-249-216-00...
- 10.0.0.50

Destinations (flow records)

- pri.authdns.ripe.n
- arin.authdns.ripe
- ns.ripe.net
- f.in-addr-servers.a...
- apnic.authdns.ripe...
- lacnic.authdns.rip...

Destination Ports (flow records)

- dns (UDP/53)
- ICMP/8
- dns (TCP/53)



kibana

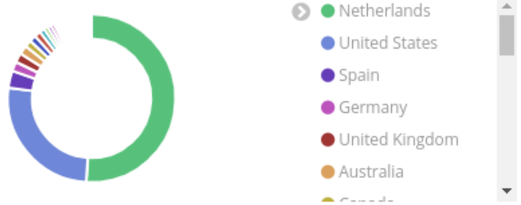
event.type: "ipfix" | node.hostname: "10.0.0.1" | Public | Add a filter + | Actions

Overview | **Top-N** | **Threats** | **Flows** | **Geo IP** | **AS Traffic** | **Exporters** | **Traffic Details** | **Flow Records**

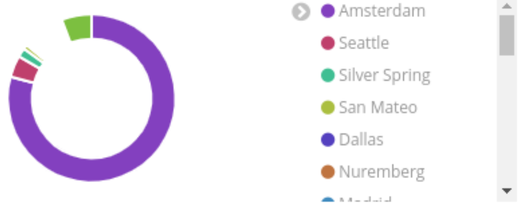
Client/Server | **Src/Dst**

ElastiFlow

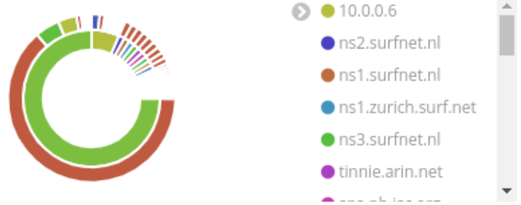
Countries (flow records)



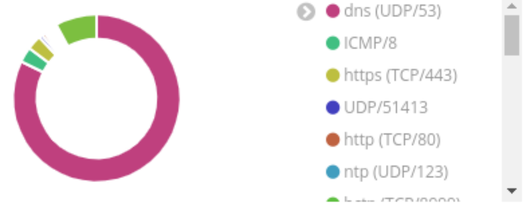
Cities (flow records)



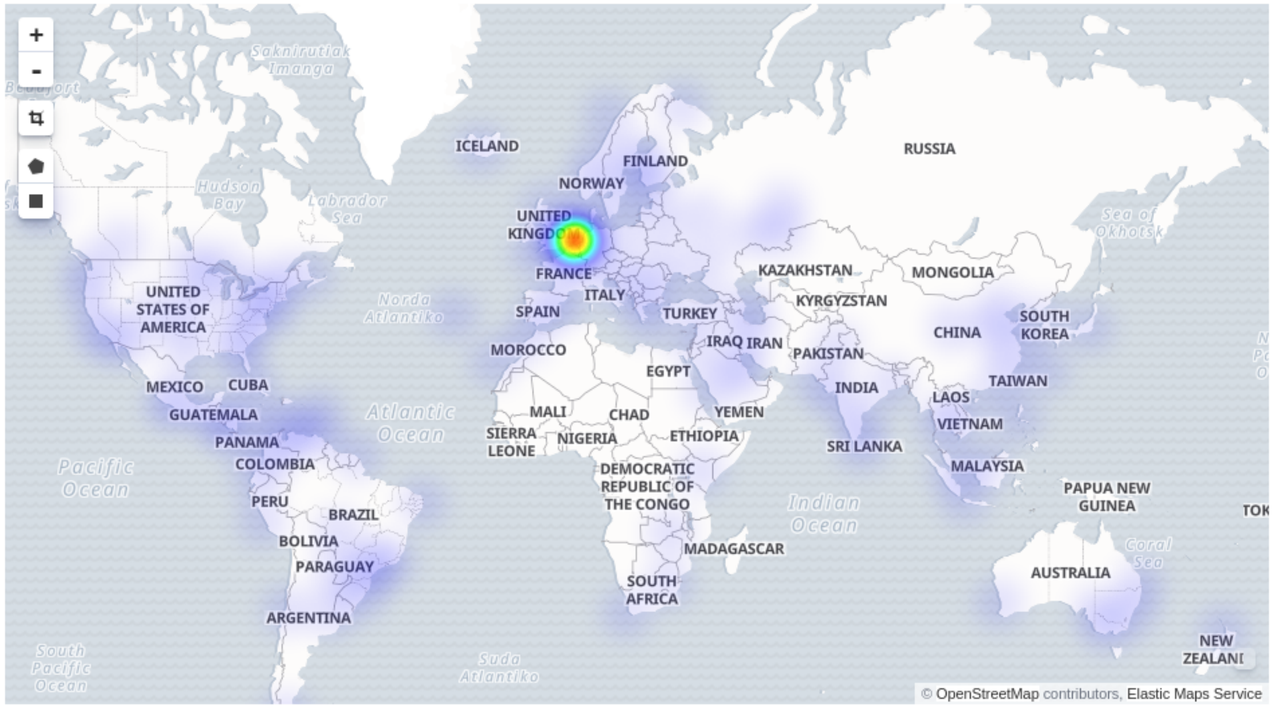
Servers and Clients (flow records)



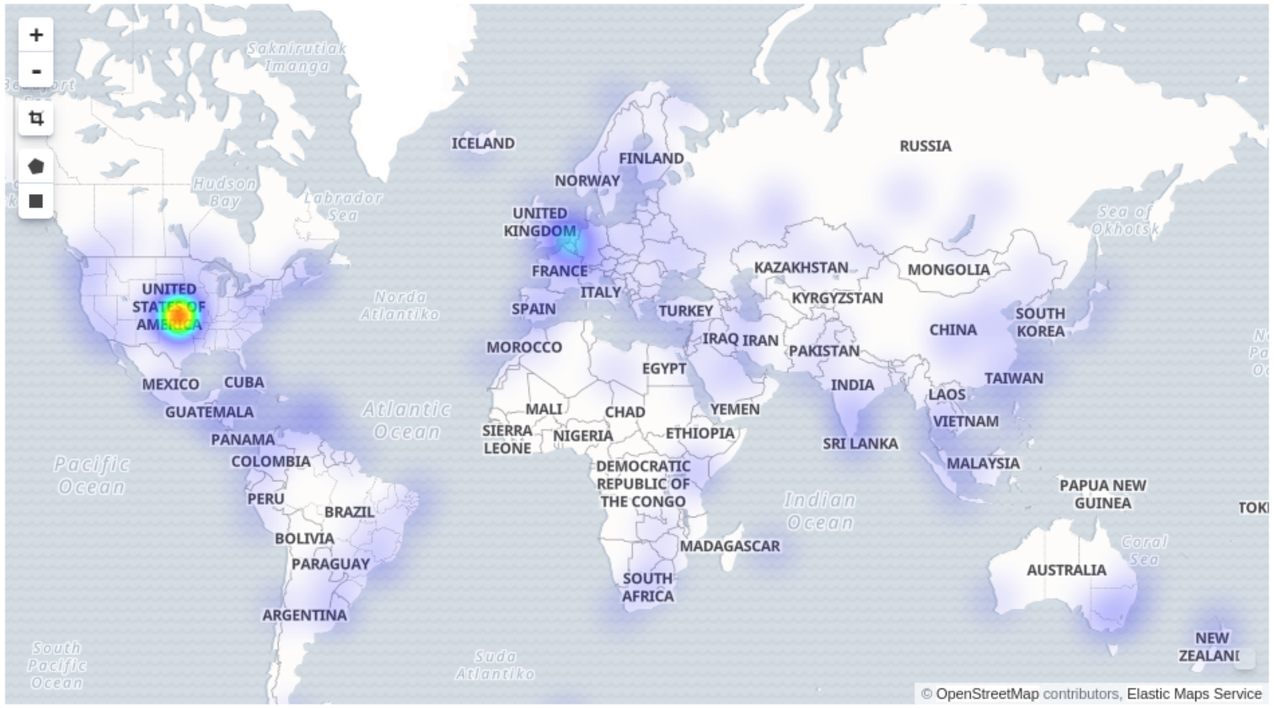
Services (flow records)



Client Locations (flow records)



Server Locations (flow records)



kibana

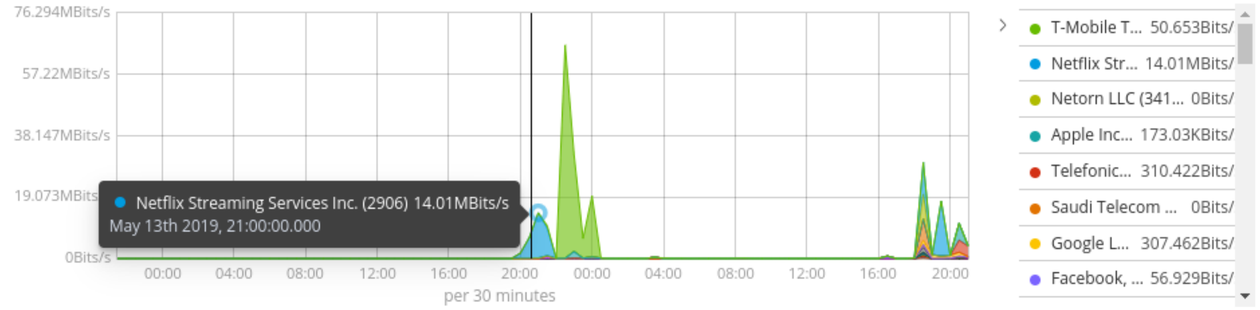
Flow Exporter: 10.0.0.1

Source AS: Select...

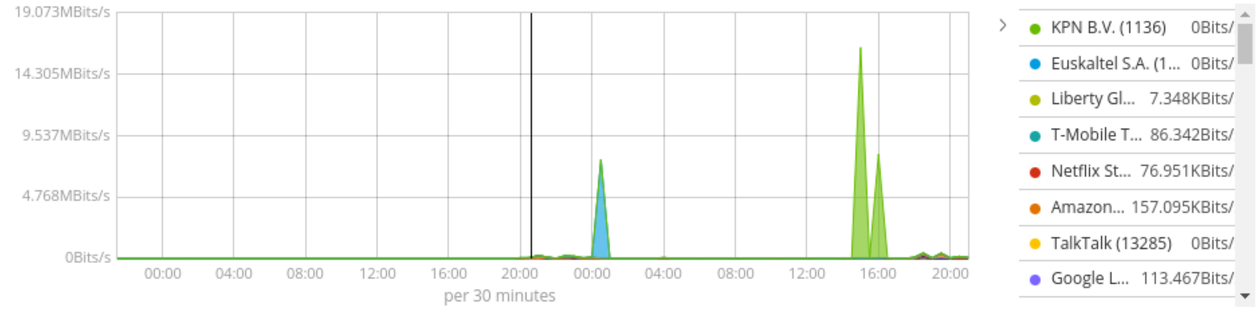
Destnation AS: Select...

Service: Select...

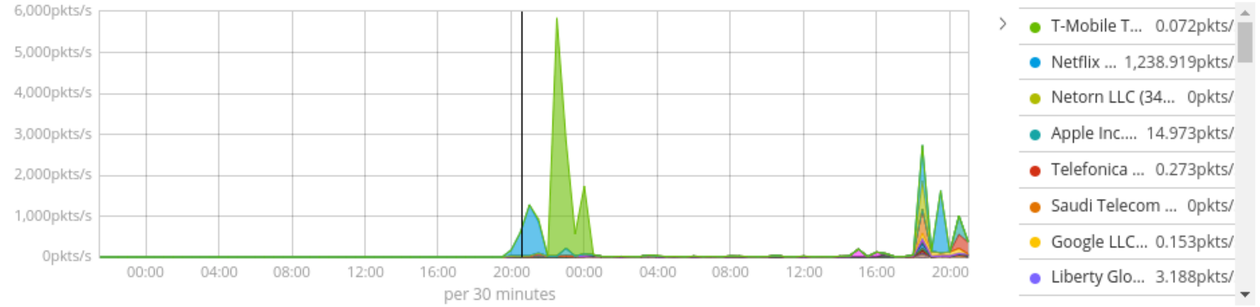
Source Autonomous Systems (bits/s)



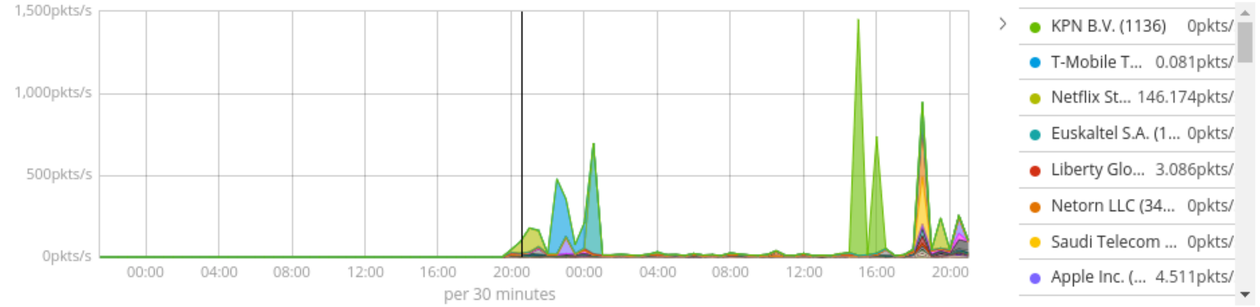
Destination Autonomous Systems (bits/s)



Source Autonomous Systems (pkts/s)

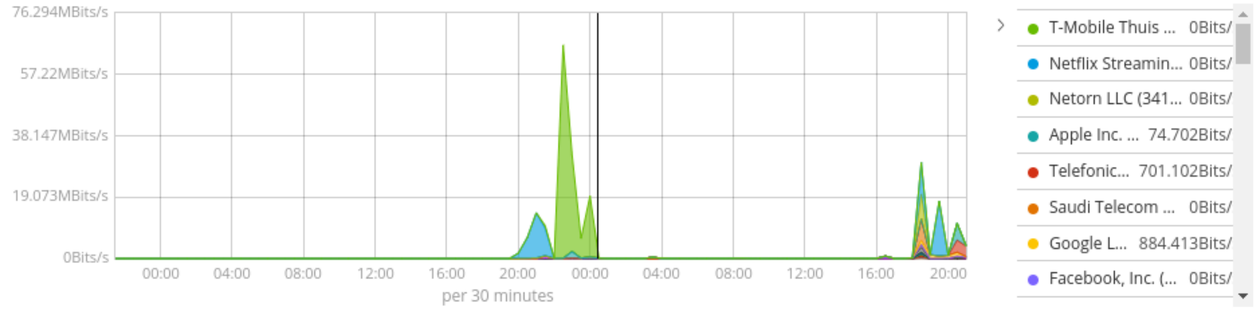


Destination Autonomous Systems (pkts/s)

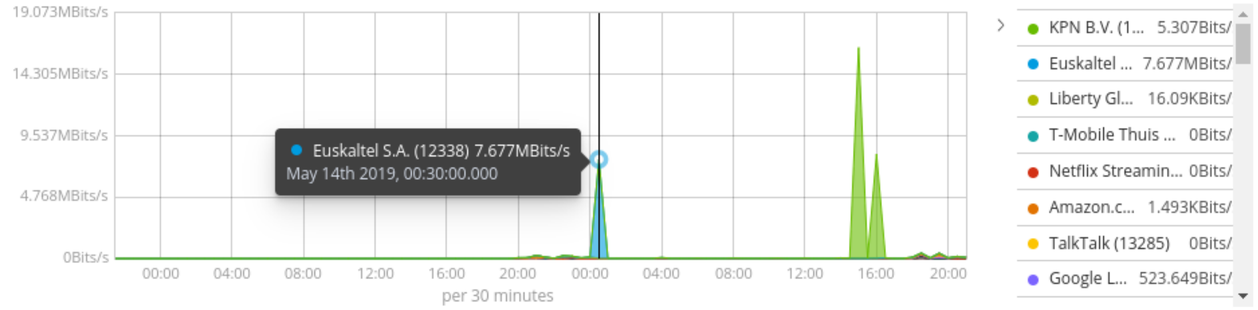


Flow Exporter: 10.0.0.1 | Source AS: Select... | Destnation AS: Select... | Service: Select...

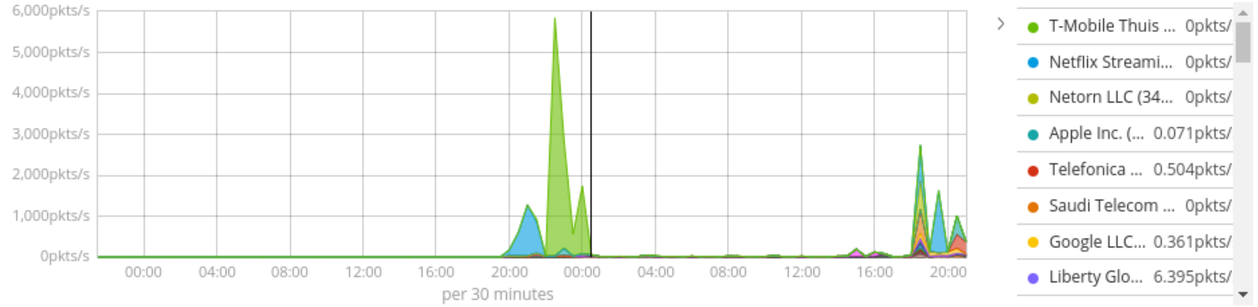
Source Autonomous Systems (bits/s)



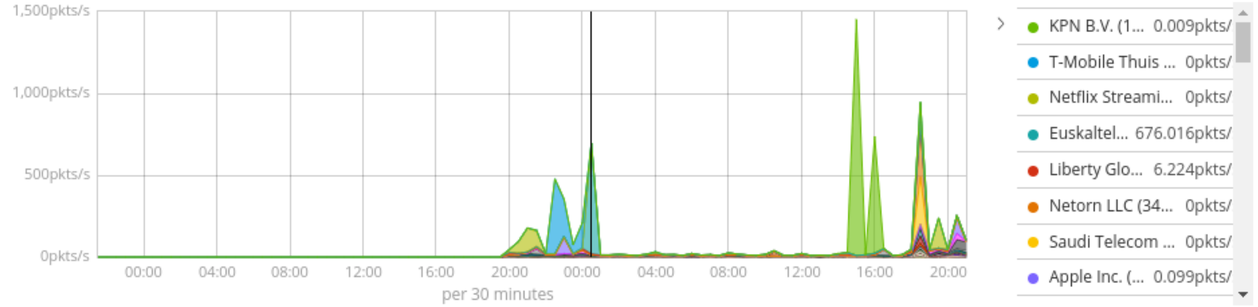
Destination Autonomous Systems (bits/s)



Source Autonomous Systems (pkts/s)



Destination Autonomous Systems (pkts/s)



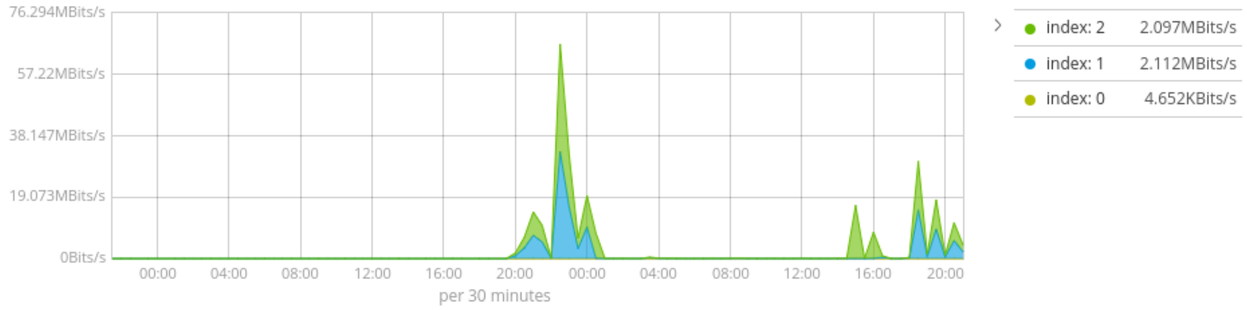
Flow Type: ipfix

Flow Exporter: 10.0.0.1

Ingress Interface: Select...

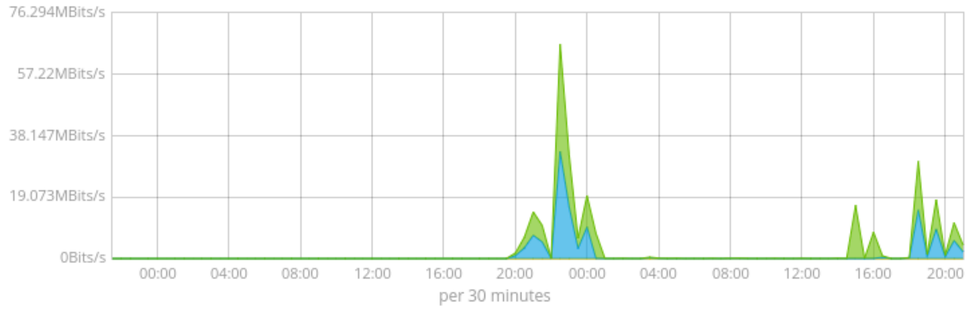
Egress Interface: Select...

Ingress Interfaces (bits/s)



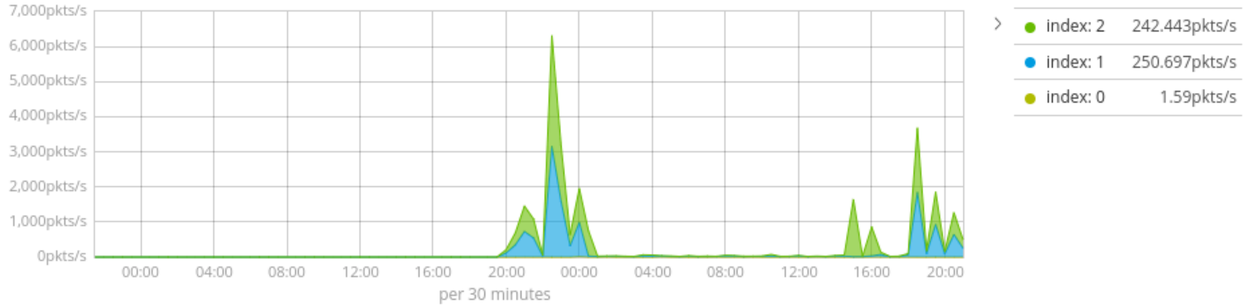
index: 2	2.097MBits/s
index: 1	2.112MBits/s
index: 0	4.652KBits/s

Egress Interfaces (bits/s)



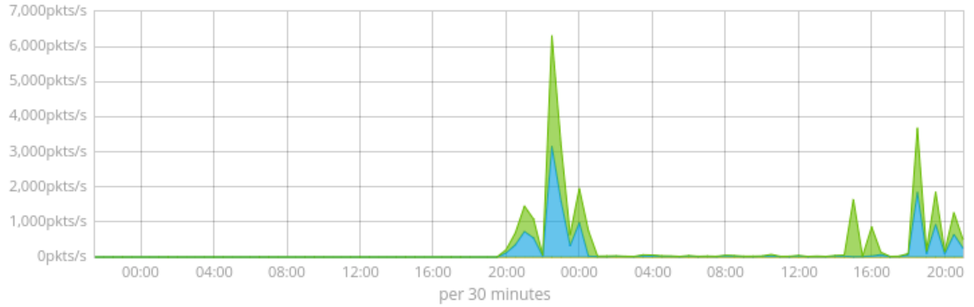
index: 2	2.1MBits/s
index: 1	2.112MBits/s
index: 0	799.747Bits/s

Ingress Interfaces (pkts/s)



index: 2	242.443pkts/s
index: 1	250.697pkts/s
index: 0	1.59pkts/s

Egress Interfaces (pkts/s)



index: 2	243.116pkts/s
index: 1	251.033pkts/s
index: 0	0.582pkts/s

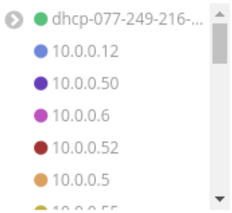
Client: Select...

Server: Select...

Service: Select...

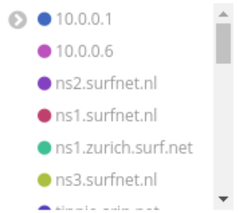
Application: Select...

Clients (flow records)



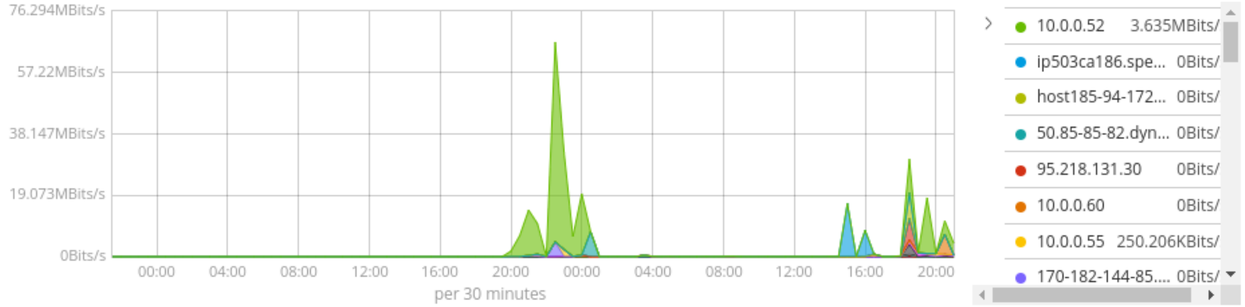
2,274
Clients

Servers (flow records)

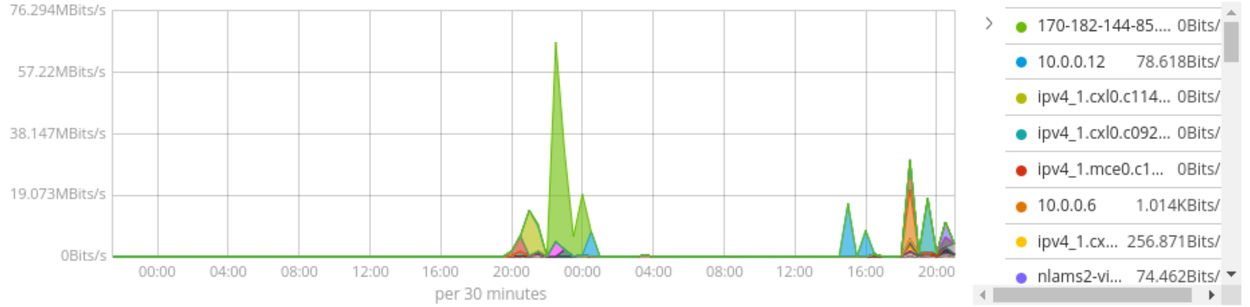


10,359
Servers

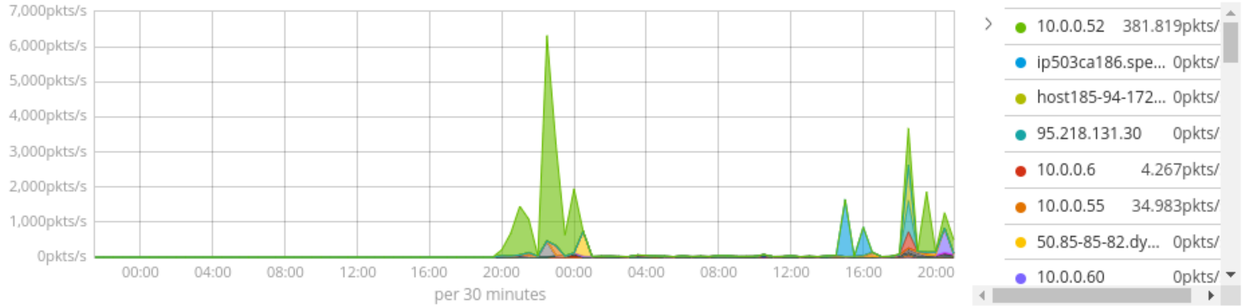
Clients (bits/s)



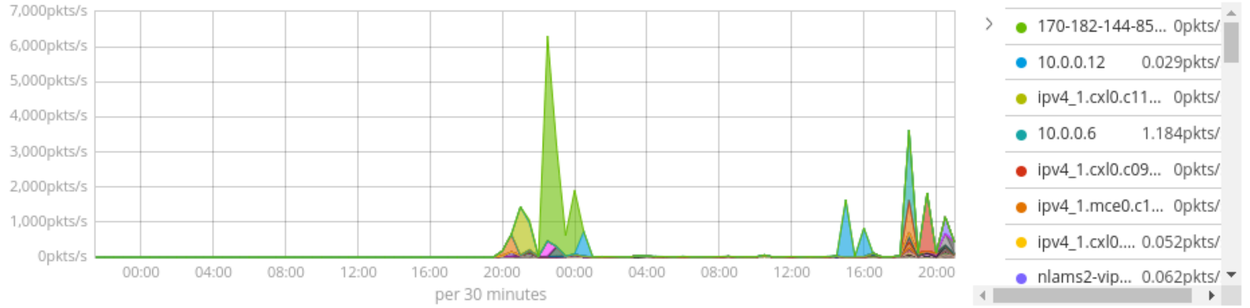
Servers (bits/s)



Clients (pkts/s)



Servers (pkts/s)



ecords)

Applications (flow records)

Client: Select...

Server: Select...

Service: Select...

Application: Select...

Filtering occurs on the "flow.application" field, which doesn't exist on any documents in the "elastiflow-*" index pattern. Choose a different field or index documents that contain values for this field.

Clients (flow records)

dhcp-077-249-216-...
10.0.0.12
10.0.0.50
10.0.0.6
10.0.0.52
10.0.0.5

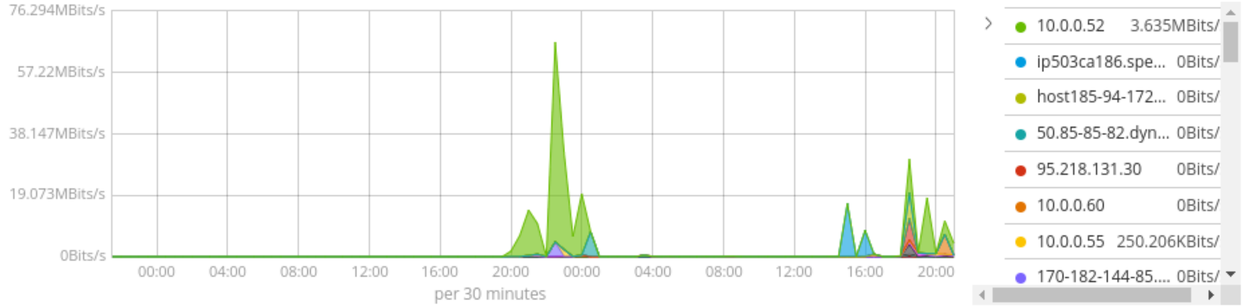
2,274
Clients

Servers (flow records)

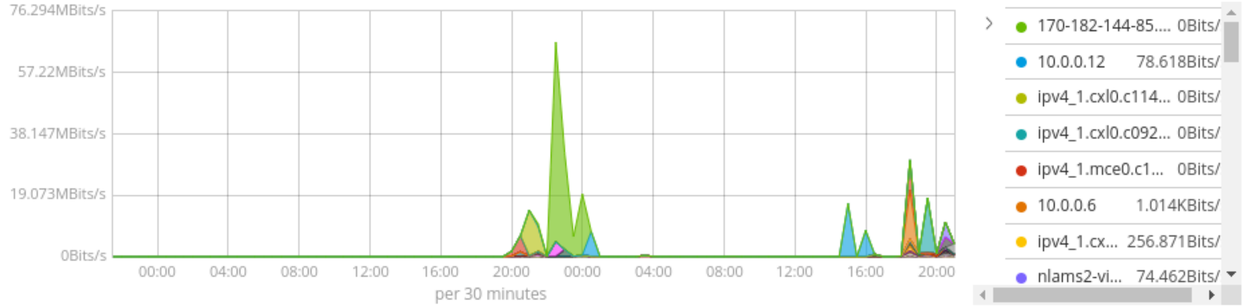
ns1.zurich.surf.net
ns3.surfnet.nl

10,359
Servers

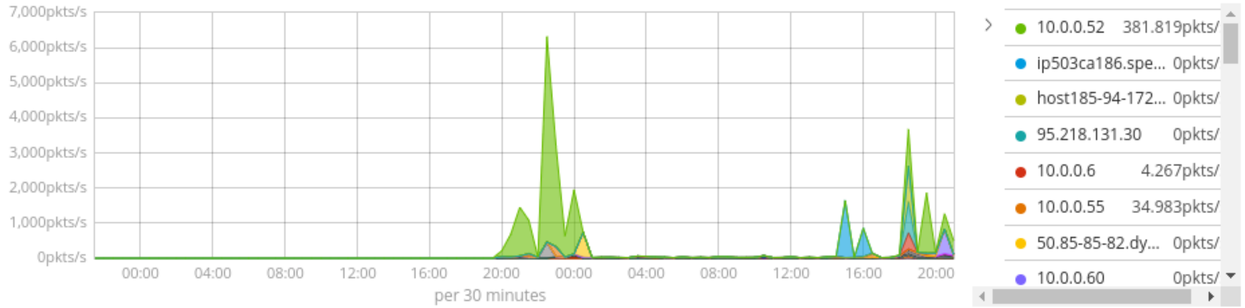
Clients (bits/s)



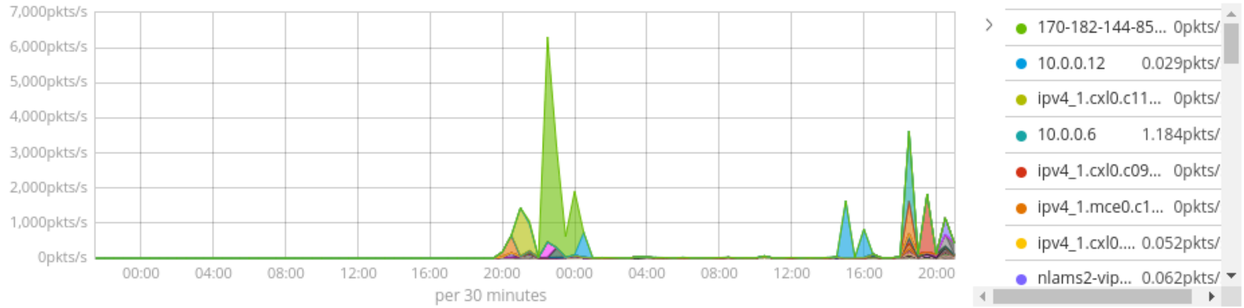
Servers (bits/s)



Clients (pkts/s)



Servers (pkts/s)



ecords)

Applications (flow records)

IP Protocol: Select...

VLAN: Select...

Type of Service: Select...

TCP Flag: Select...

Filtering occurs on the "flow.tcp_flags" field, which doesn't exist on any documents in the "elastiflow-*" index pattern. Choose a different field or index documents that contain values for this field.

IP Protocols (flow records)

UDP
TCP
ICMP
IGMP

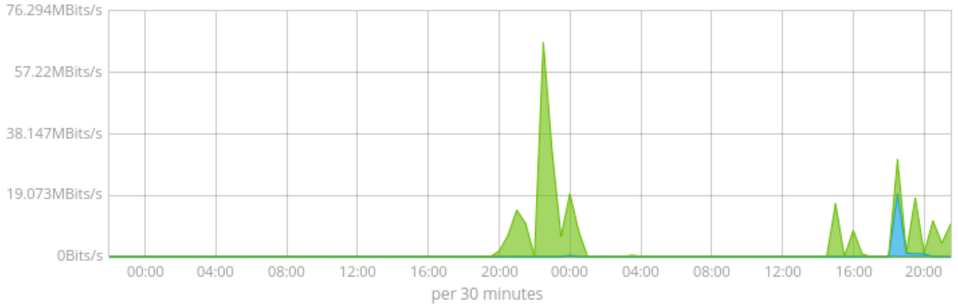
4
IP Protocols

VLANs (flow records)

No results found

0
VLANs

IP Protocols (bits/s)

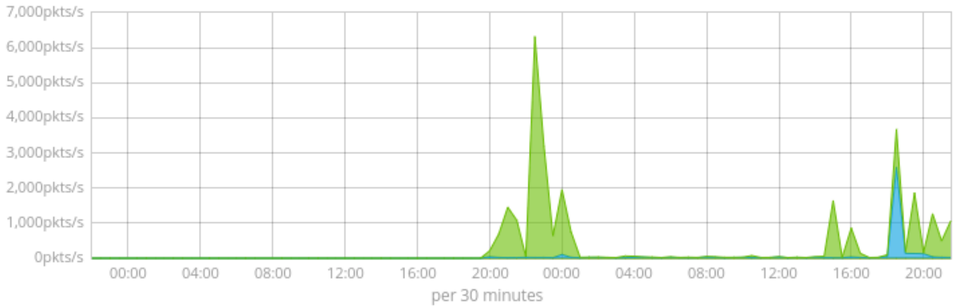


TCP	10.034MBits/s
UDP	25.496KBits/s
ICMP	1.304KBits/s
IGMP	0Bits/s

VLANs (bits/s)

No data to display for the selected metrics

IP Protocols (pkts/s)



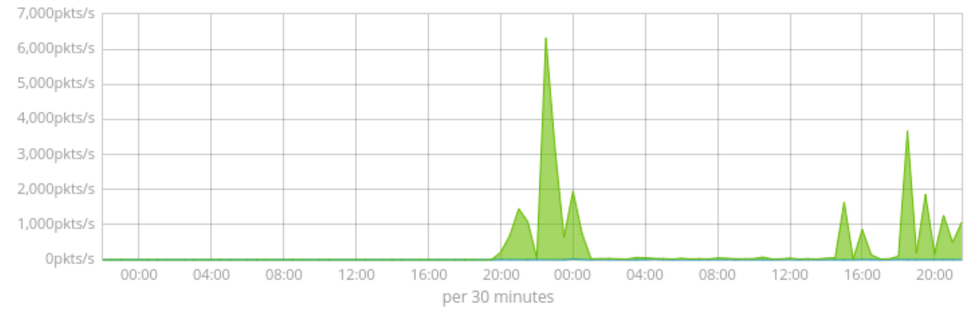
TCP	1,035.766pkts/s
UDP	19.214pkts/s
ICMP	2.291pkts/s
IGMP	0pkts/s

VLANs (pkts/s)

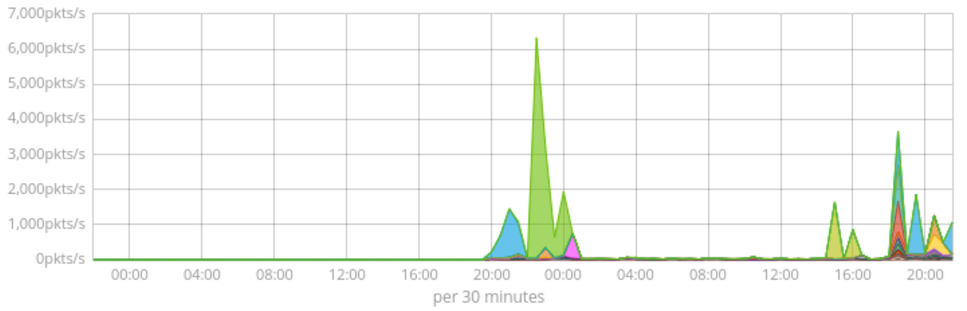
No data to display for the selected metrics

(flow records)

TCP Flags (flow records)



public	1,058.634pkts/s
private	4.844pkts/s



T-Mobile Thuis ...	0pkts/
Netflix St...	918.477pkts/
KPN B.V. (1...	0.034pkts/
Netorn LLC (34...	0pkts/
Saudi Telecom ...	0pkts/
Apple Inc. (...	0.243pkts/
Telefonica ...	0.752pkts/
Liberty Gl...	12.545pkts/

Countries (flow records)

Netherlands
United States
Spain
United Kingdom
Germany
Australia

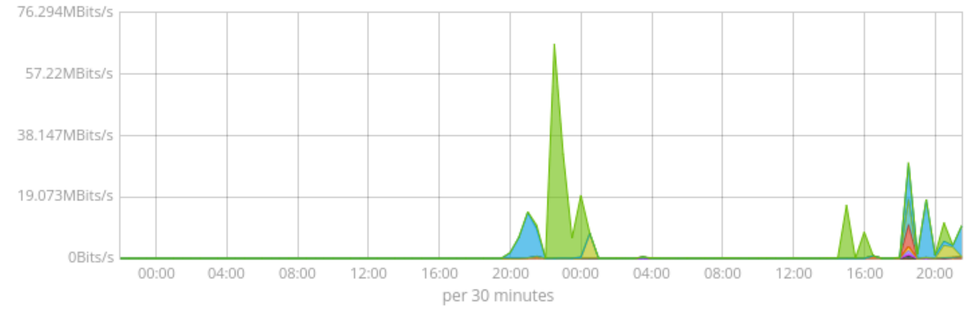
104
Countries

Cities (flow records)

Amsterdam
Seattle
Silver Spring
San Mateo
Dallas
Nuremberg

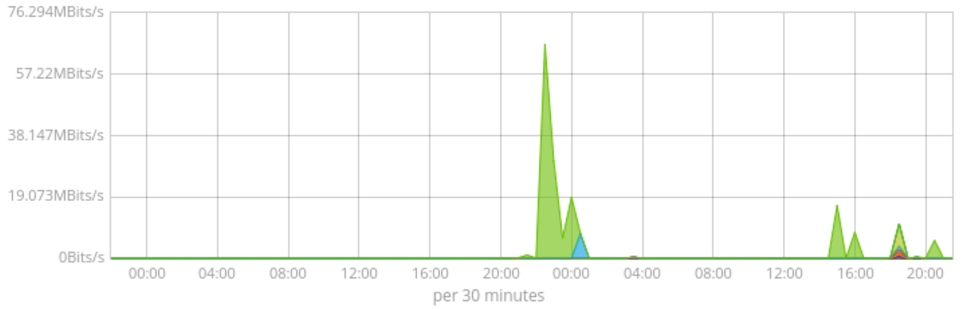
1,460
Cities

Countries (bits/s)



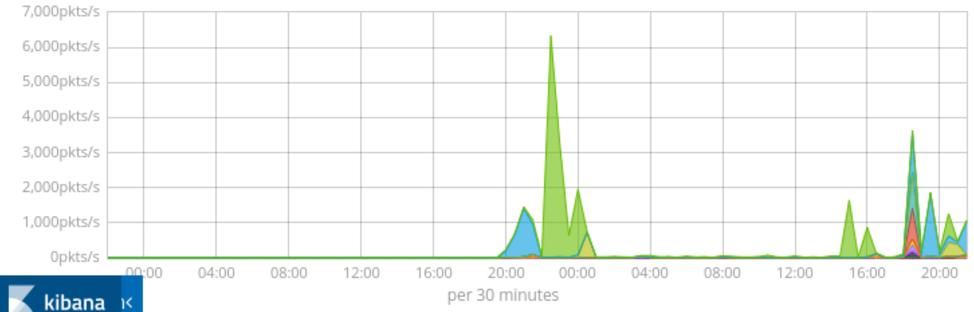
Netherla...	125.78KBits/
United St...	9.422MBits/
Spain	1.997KBits/
Russia	166.853Bits/
Saudi Arabia	0Bits/
Ireland	559.466KBits/
United Kin...	6.362KBits/
Canada	174.027Bits/

Cities (bits/s)



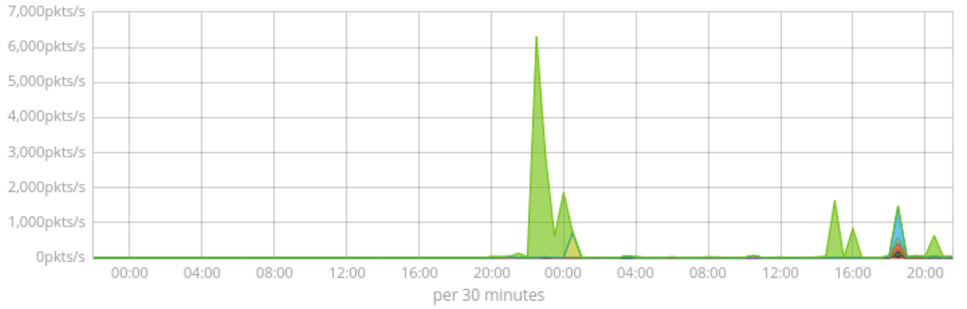
Amster...	117.724KBits/
Bermeo	0Bits/
Riyadh	0Bits/
Pierrefonds	1.138Bits/
Penzance	0Bits/
Dublin	22.98KBits/
Singapore	62.436Bits/
London	5.272KBits/

Countries (pkts/s)



Netherlan...	30.096pkts/
United S...	946.557pkts/
Spain	2.011pkts/
Russia	0.158pkts/
Saudi Arabia	0pkts/
Ireland	83.07pkts/
United Kin...	1.638pkts/
Canada	0.177pkts/

Cities (pkts/s)



Amsterdam	25.791pkts/
Riyadh	0pkts/
Bermeo	0pkts/
Penzance	0pkts/
Pierrefonds	0.002pkts/
Dublin	3.701pkts/
Utrecht	0.008pkts/
Naaldwijk	1.148pkts/

ElastiFlow

Flow Type

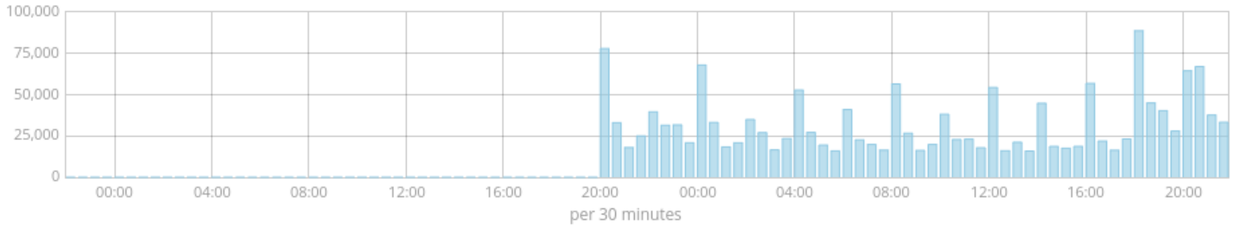
ipfix

Flow Exporter

10.0.0.1

Flow Records

1,686,376



ipfix 33,306

1–50 of 1,689,548

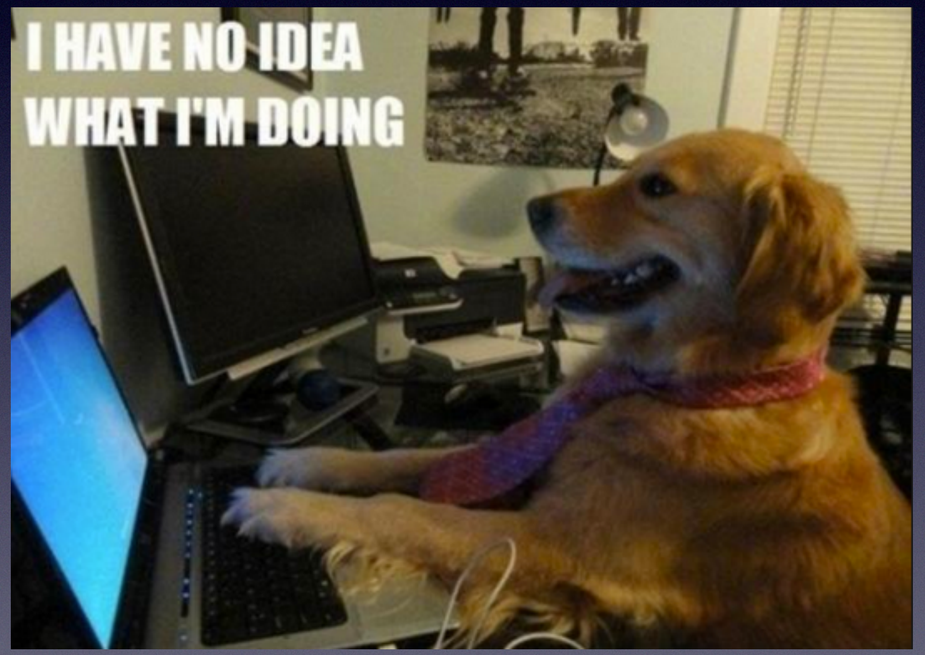
Time	node.hostname	flow.client_hostname	flow.server_hostname	flow.service_name	flow.bytes	flow.packets
May 14th 2019, 22:03:01.000	10.0.0.1	10.0.0.50	h.root-servers.net	dns (UDP/53)	98B	1
May 14th 2019, 22:03:01.000	10.0.0.1	10.0.0.12	10.0.0.1	dns (UDP/53)	108B	1
May 14th 2019, 22:03:01.000	10.0.0.1	dhcp-077-249-216-006.chello.nl	a2-22-230-192.deploy.static.akamaitechnologies.com	dns (UDP/53)	95B	1
May 14th 2019, 22:03:01.000	10.0.0.1	10.0.0.50	l.root-servers.net	dns (UDP/53)	60B	1
May 14th 2019, 22:03:01.000	10.0.0.1	10.0.0.50	e.root-servers.net	dns (TCP/53)	339B	6
May 14th 2019, 22:03:01.000	10.0.0.1	dhcp-077-249-216-006.chello.nl	ns-620.awsdns-13.net	dns (UDP/53)	85B	1
May 14th 2019, 22:03:01.000	10.0.0.1	10.0.0.50	e.root-servers.net	dns (TCP/53)	339B	6
May 14th 2019, 22:03:01.000	10.0.0.1	dhcp-077-249-216-006.chello.nl	nsa.online.net	dns (UDP/53)	79B	1
May 14th 2019, 22:03:01.000	10.0.0.1	10.0.0.50	d.root-servers.net	dns (TCP/53)	339B	6
May 14th 2019, 22:03:01.000	10.0.0.1	10.0.0.12	10.0.0.1	dns (UDP/53)	122B	1
May 14th 2019, 22:03:01.000	10.0.0.1	10.0.0.12	10.0.0.1	dns (UDP/53)	72B	1
May 14th 2019, 22:03:01.000	10.0.0.1	dhcp-077-249-216-006.chello.nl	a95-100-168-194.deploy.static.akamaitechnologies.com	dns (UDP/53)	78B	1
May 14th 2019, 22:03:01.000	10.0.0.1	10.0.0.50	h.root-servers.net	dns (UDP/53)	98B	1
May 14th 2019, 22:03:01.000	10.0.0.1	dhcp-077-249-216-006.chello.nl	10-33-15-51.rev.cloud.scaleway.com	dns (UDP/53)	201B	1

La *no* demo 🤡

- ¿Cuánto me va a costar? Un *pico*… en hardware
  - http://bit.ly/esnog23-elastiflow-resource-usage

¿Preguntas?

- http://bit.ly/esnog23-elastiflow-origin
- http://bit.ly/esnog23-elastiflow-home
- http://bit.ly/esnog23-elastiflow-resource-usage
- http://bit.ly/esnog23-openhrc



¡Muchas gracias!

\(^o^)/

Diapositivas adicionales

- Muestra de índices en elasticsearch

```
green open elastiflow-3.4.1-2019.05.13 XxNcxjlzQ2qy5YhQqRY2yw 1 0  418054 0 136.2mb 136.2mb
green open elastiflow-3.4.1-2019.05.14 8JvbqaRHQJuHJMQ6bhzrCg 1 0 1538696 0 485.5mb 485.5mb
green open elastiflow-3.4.1-2019.05.15 bHwVVn7xR_2c6oOKU8sNyQ 1 0  776897 0 327.2mb 327.2mb
```

Diapositivas adicionales

- Muestra de documento en elasticsearch


```
{
  "node" : {
    "hostname" : "10.0.0.1",
    "ipaddr" : "10.0.0.1"
  },
  "ipfix" : {
    "octetDeltaCount" : 75,
    "flowStartMilliseconds" : "2019-05-15T00:01:01.000Z",
    "flowset_id" : 256,
    "flowEndMilliseconds" : "2019-05-15T00:01:01.000Z",
    "packetDeltaCount" : 1,
    "version" : 10
  },
  "event" : {
    "host" : "10.0.0.1",
    "type" : "ipfix"
  },
  "flow" : {
    "src_geo_location" : {
      "lon" : 4.8669,
      "lat" : 52.3617
    },
    "dst_port" : 53,
    "ip_version" : "IPv4",
    "output_snmp" : 1,
    "city" : "Amsterdam",
    "service_port" : "53",
    "client_hostname" : "dhcp-077-249-216-006.chello.nl",
    "src_port_name" : "UDP/14257",
    "direction" : "unspecified",
    "dst_hostname" : "a2-16-40-192.deploy.static.akamaitechnologies.com",
    "country_code" : "NL",
    "dst_geo_location" : {
      "lon" : 8.0,
      "lat" : 47.0
    },
```

```
    "server_hostname" : "a2-16-40-192.deploy.static.akamaitechnologies.com",
    "input_ifname" : "index: 1",
    "server_autonomous_system" : "Akamai International B.V. (21342)",
    "client_asn" : "6830",
    "src_city" : "Amsterdam",
    "client_country_code" : "NL",
    "autonomous_system" : [
      "Akamai International B.V. (21342)",
      "Liberty Global B.V. (6830)"
    ],
    "src_addr" : "77.249.216.6",
    "ip_protocol" : "UDP",
    "src_country_code" : "NL",
    "country" : "Netherlands",
    "src_autonomous_system" : "Liberty Global B.V. (6830)",
    "client_autonomous_system" : "Liberty Global B.V. (6830)",
    "dst_autonomous_system" : "Akamai International B.V. (21342)",
    "server_asn" : "21342",
    "src_asn" : 6830,
    "client_country" : "Netherlands",
    "server_geo_location" : "47.0,8.0",
    "src_hostname" : "dhcp-077-249-216-006.chello.nl",
    "server_addr" : "2.16.40.192",
    "dst_addr" : "2.16.40.192",
    "packets" : "1",
    "traffic_locality" : "public",
    "client_geo_location" : "52.3617,4.8669",
    "output_ifname" : "index: 1",
    "tos" : 0,
    "bytes" : 75,
    "dst_port_name" : "dns (UDP/53)",
    "src_country" : "Netherlands",
    "input_snmp" : 1,
    "dst_asn" : 21342,
    "service_name" : "dns (UDP/53)",
    "client_addr" : "77.249.216.6",
    "client_city" : "Amsterdam",
    "src_port" : 14257
  },
  "@version" : "3.4.1",
  "@timestamp" : "2019-05-15T00:01:44.000Z"
}
```