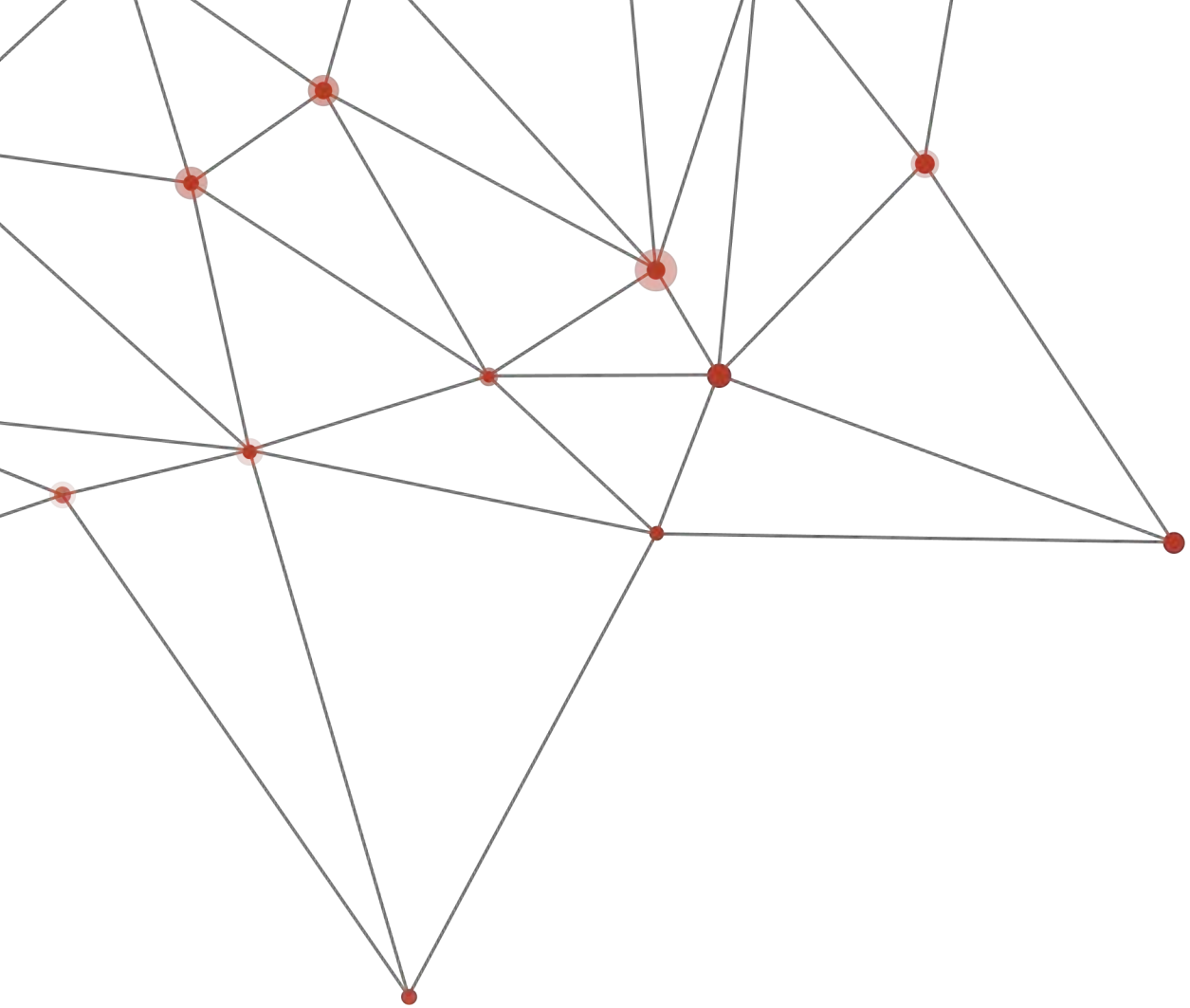


How we built sFlow visualization tool (open source)

Blažej Krajňák

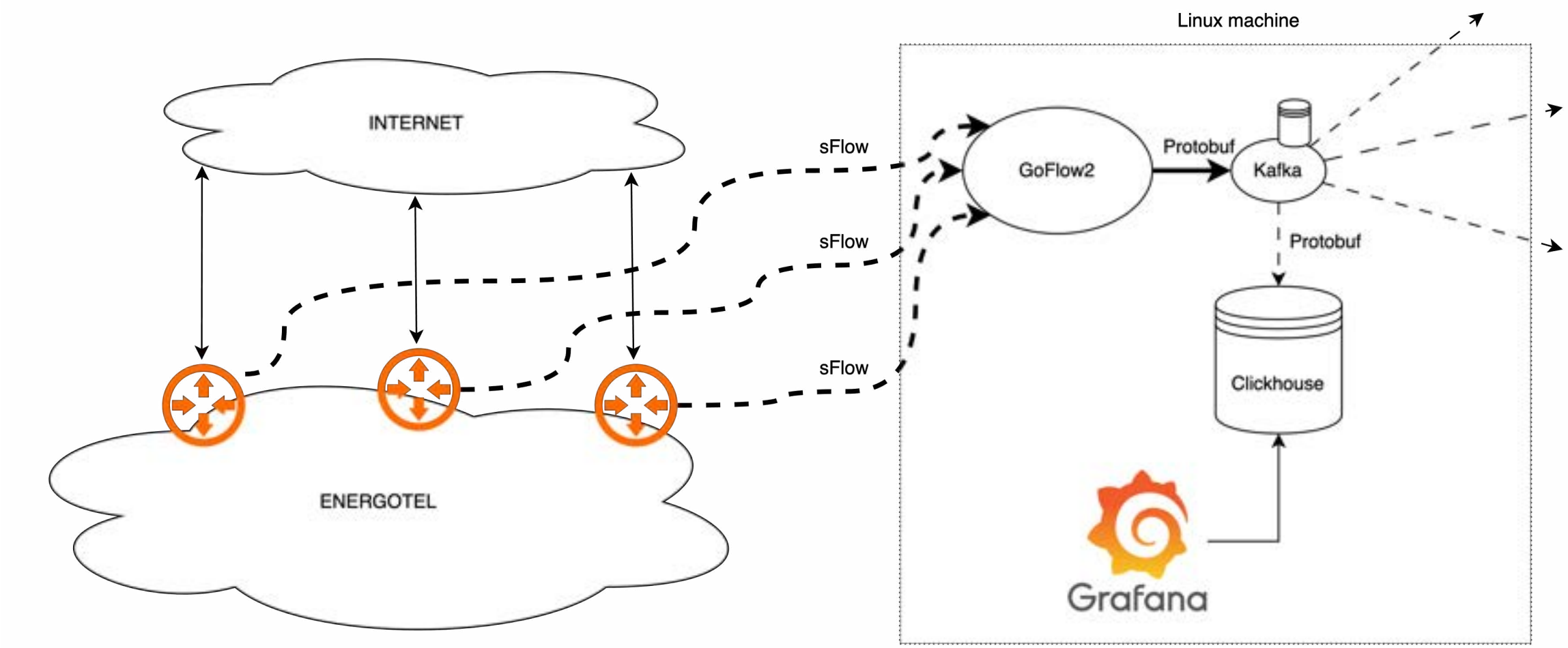
CSNOG | 22.1.2025

Energotel, a.s.

- provides B2B services
- national optical fiber network (400G backbone)
- internet services, L2 / L3 services
- lease of dark fibers / lambdas
- IT outsourcing
- 24/7 NOC and SOC
- cyber security audits and trainings
- part of critical national infrastructure

This comes soon …

… but theory first – how the tool works



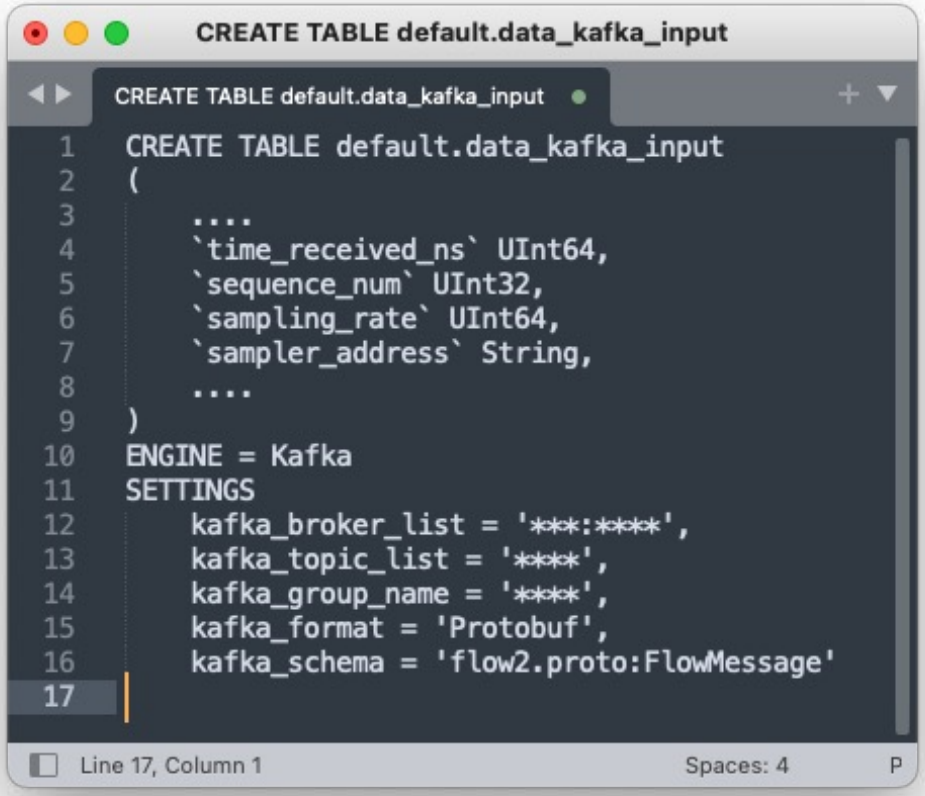
Clickhouse

- column-oriented database management system
- data compression by default
- provides automatic data aggregation (materialized view)

Provides many nice features:

Clickhouse – Kafka connector

- reads and saves data from Kafka
- auto-parse protobuf (binary) data to structure



Clickhouse – create table from online data

CREATE TABLE default.iana_protocols

CREATE TABLE default.iana_protocols

```
CREATE TABLE default.iana_protocols
(
    `Decimal` String,
    `Keyword` String,
    `Protocol` String,
    `IPv6ExtensionHeader` String,
    `Reference` String
)
ENGINE = URL('https://www.iana.org/assignments/
protocol-numbers/protocol-numbers-1.csv', 'CSV')
SETTINGS input_format_csv_skip_first_lines = 1

```

Line 11, Column 1 Spaces: 4 Plain Text

CREATE TABLE default.geoip

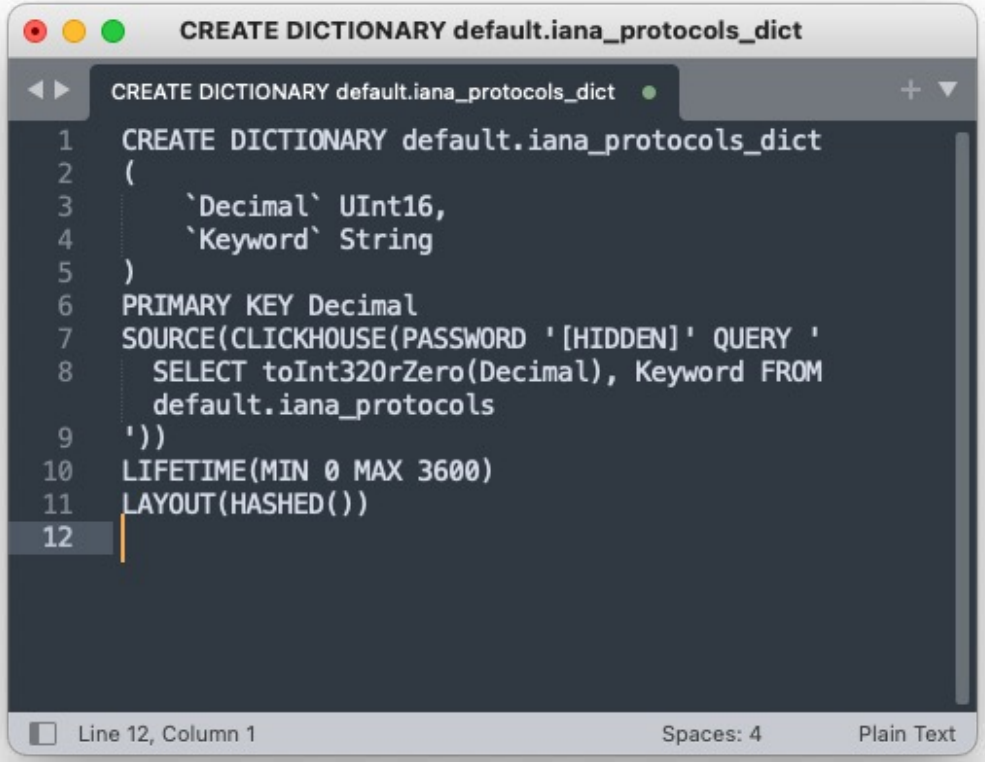
CREATE TABLE default.geoip

```
CREATE TABLE default.geoip
(
    `ip_range_start` IPv4,
    `ip_range_end` IPv4,
    `country_code` Nullable(String),
    `state1` Nullable(String),
    `state2` Nullable(String),
    `city` Nullable(String),
    `postcode` Nullable(String),
    `latitude` Float64,
    `longitude` Float64,
    `timezone` Nullable(String)
)
ENGINE = URL('https://raw.githubusercontent.com/
sapics/ip-location-db/master/dbip-city/
dbip-city-ipv4.csv.gz', 'CSV')

```

Line 15, Column 1 Spaces: 4 Plain Text

Clickhouse – dictionaries

- small tables kept in RAM



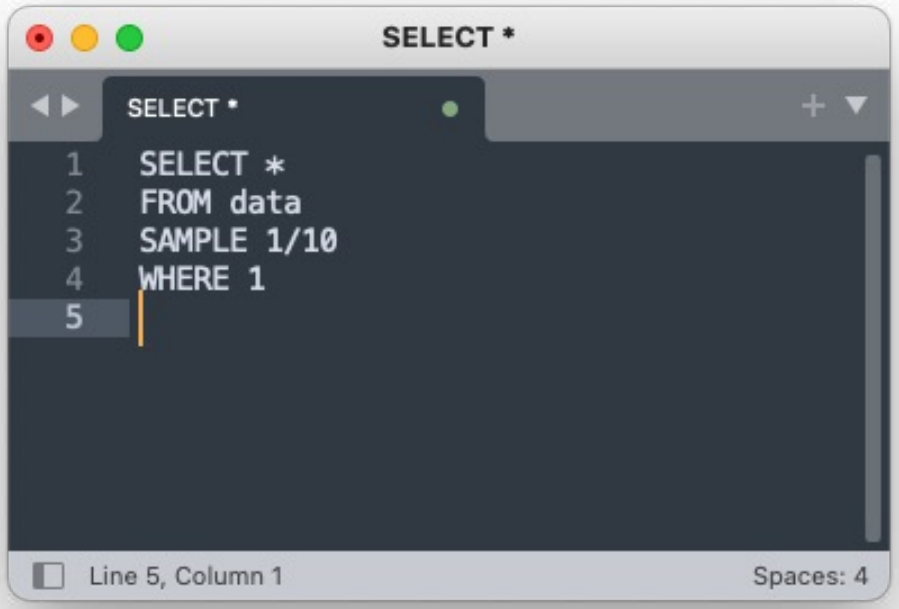
Clickhouse – ALIAS data type

CREATE TABLE default.data

```
CREATE TABLE default.data
(
    ....
    `ip_flags` UInt32,
    `tcp_flags` UInt32,

    `tcp_flag_fin` Bool ALIAS bitTest(tcp_flags, 0),
    `tcp_flag_syn` Bool ALIAS bitTest(tcp_flags, 1),
    `tcp_flag_rst` Bool ALIAS bitTest(tcp_flags, 2),
    `tcp_flag_psh` Bool ALIAS bitTest(tcp_flags, 3),
    `tcp_flag_ack` Bool ALIAS bitTest(tcp_flags, 4),
    `tcp_flag_urg` Bool ALIAS bitTest(tcp_flags, 5),
    `tcp_flag_ecn_echo` Bool ALIAS bitTest(tcp_flags, 6),
    `tcp_flag_cw_reduced` Bool ALIAS bitTest(tcp_flags, 7),
    `tcp_flag_acc_ecn` Bool ALIAS bitTest(tcp_flags, 8),

    `ip_flag_more_fragments` Bool ALIAS bitTest(ip_flags, 0),
    `ip_flag_dont_fragment` Bool ALIAS bitTest(ip_flags, 1),
    `ip_flag_reserved_bit` Bool ALIAS bitTest(ip_flags, 2),

    `src_as_name` String ALIAS concat('AS', src_as, ' - ', dictGetOrDefault(default.asn_dict, 'asn_name', src_as, 'Unknown')),
    `dst_as_name` String ALIAS concat('AS', dst_as, ' - ', dictGetOrDefault(default.asn_dict, 'asn_name', dst_as, 'Unknown')),
    `in_if_name` String ALIAS dictGetOrDefault(default.engt_ifaces_dict, 'ifDescription', (sampler_ip, in_if), concat(sampler_ip, '-', in_if)),
    `out_if_name` String ALIAS dictGetOrDefault(default.engt_ifaces_dict, 'ifDescription', (sampler_ip, out_if), concat(sampler_ip, '-', out_if)),
    `etype_name` String ALIAS dictGetOrDefault(default.ethertypes_dict, 'Keyword', etype, etype),
    `proto_name` String ALIAS dictGetOrDefault(default.iana_protocols_dict, 'Keyword', proto, proto),
    `src_mac_name` String ALIAS MACNumToString(src_mac),
    `dst_mac_name` String ALIAS MACNumToString(dst_mac),
    `ip_dscp` UInt32 ALIAS bitShiftRight(ip_tos, 2),
    `dir_in` Bool ALIAS dictHas(default.engt_ifaces_dict, (sampler_ip, in_if)),
    `dir_out` Bool ALIAS dictHas(default.engt_ifaces_dict, (sampler_ip, out_if)),
    ....
)
```

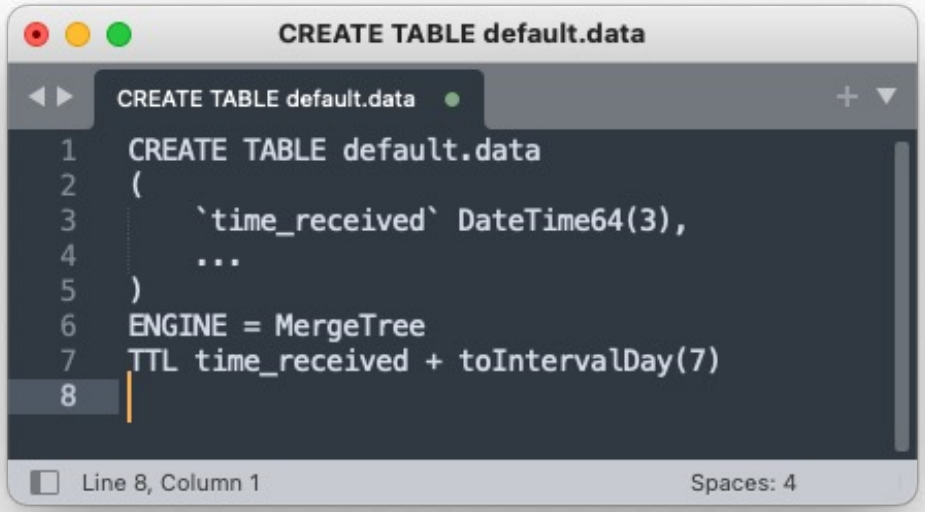
Clickhouse – SAMPLE function

- performs query on fraction of data (1/n)
- helps to speed up query (where suitable)
- it‘s a deterministic mechanism
- need to specify sampling key on table creation



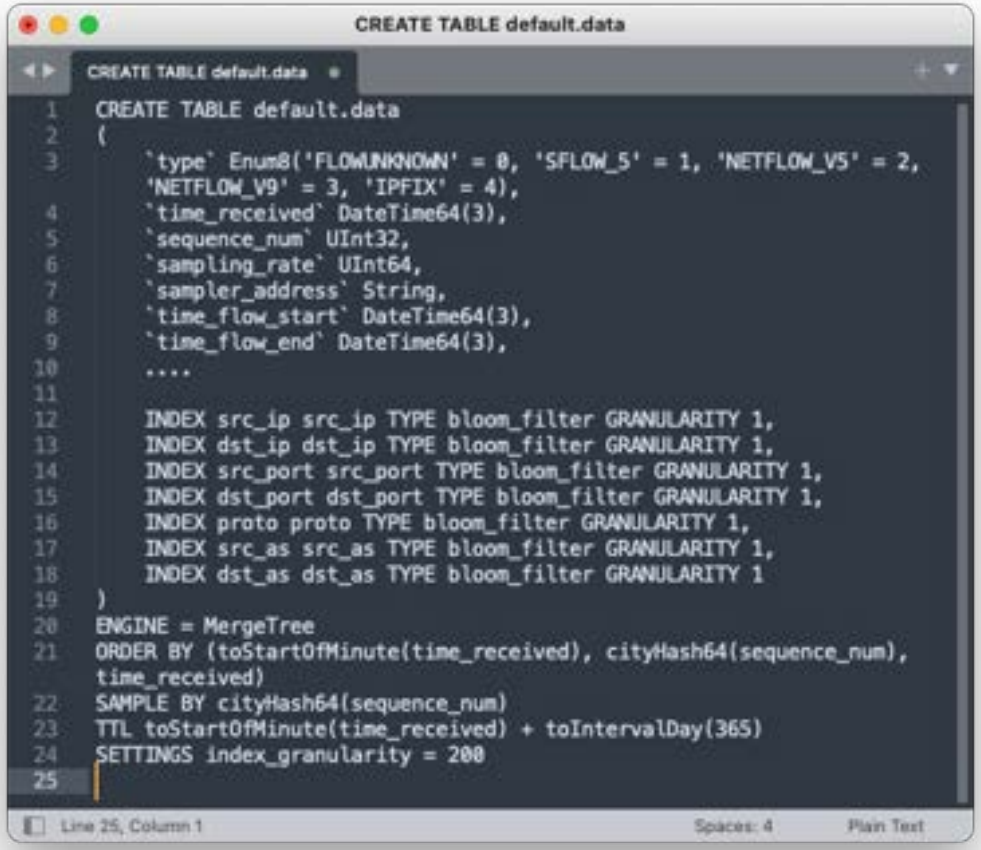
Clickhouse – auto data removal

- ability to specify data lifetime



Clickhouse – the main data table tuning

- sampling key needs to be random INT value –> use hash
- sampling key needs to be present in primary key (= ORDER BY if not specified)
- filtering by time range is more important than sampling key –> use „time_received“ before sampling key in primary key
- put only low-cardinality columns before sampling expression in primary key -> use toStartOfMinute(time_received)
- any INDEX in Clickhouse is skipping index -> use small enough granules size



Available data metrics (from GoFlow2 + computed)

`type` Enum8('FLOWUNKNOWN' = 0, 'SFLOW_5' = 1, 'NETFLOW_V5' = 2, 'NETFLOW_V9' = 3, 'IPFIX' = 4),
`time_received` DateTime64(3),
`sequence_num` UInt32,
`sampling_rate` UInt64,
`sampler_address` String,
`time_flow_start` DateTime64(3),
`time_flow_end` DateTime64(3),
`bytes` UInt64,
`packets` UInt64,
`src_addr` String,
`dst_addr` String,
`etype` UInt32,
`proto` UInt32,
`src_port` UInt32,
`dst_port` UInt32,
`in_if` UInt32,
`out_if` UInt32,
`src_mac` UInt64,
`dst_mac` UInt64,
`src_vlan` UInt32,
`dst_vlan` UInt32,
`vlan_id` UInt32,
`ip_tos` UInt32,
`forwarding_status` UInt32,
`ip_ttl` UInt32,

`ip_flags` UInt32,
`tcp_flags` UInt32,
`icmp_type` UInt32,
`icmp_code` UInt32,
`ipv6_flow_label` UInt32,
`fragment_id` UInt32,
`fragment_offset` UInt32,
`src_as` UInt32,
`dst_as` UInt32,
`next_hop` String,
`next_hop_as` UInt32,
`src_net` UInt32,
`dst_net` UInt32,
`bgp_next_hop` String,
`bgp_communities` Array(UInt32),
`as_path` Array(UInt32),
`mpls_ttl` Array(UInt32),
`mpls_label` Array(UInt32),
`mpls_ip` Array(String),
`observation_domain_id` UInt32,
`observation_point_id` UInt32,
`sampler_ip` IPv6,
`src_ip` IPv6,
`dst_ip` IPv6,
`bgp_next_hop_ip` IPv6,

`tcp_flag_fin` Bool ALIAS bitTest(tcp_flags, 0),
`tcp_flag_syn` Bool ALIAS bitTest(tcp_flags, 1),
`tcp_flag_rst` Bool ALIAS bitTest(tcp_flags, 2),
`tcp_flag_psh` Bool ALIAS bitTest(tcp_flags, 3),
`tcp_flag_ack` Bool ALIAS bitTest(tcp_flags, 4),
`tcp_flag_urg` Bool ALIAS bitTest(tcp_flags, 5),
`tcp_flag_ecn_echo` Bool ALIAS bitTest(tcp_flags, 6),
`tcp_flag_cw_reduced` Bool ALIAS bitTest(tcp_flags, 7),
`tcp_flag_acc_ecn` Bool ALIAS bitTest(tcp_flags, 8),

`ip_flag_more_fragments` Bool ALIAS bitTest(ip_flags, 0),
`ip_flag_dont_fragment` Bool ALIAS bitTest(ip_flags, 1),
`ip_flag_reserved_bit` Bool ALIAS bitTest(ip_flags, 2),

`src_as_name` String ALIAS concat('AS', src_as, ' - ', dictGetOrDefault(default.asn_dict, 'asn_name', src_as, 'Unknown')),
`dst_as_name` String ALIAS concat('AS', dst_as, ' - ', dictGetOrDefault(default.asn_dict, 'asn_name', dst_as, 'Unknown')),

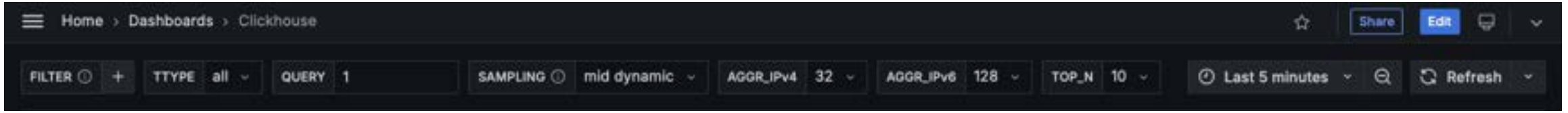
`in_if_name` String ALIAS dictGetOrDefault(default.engt_ifaces_dict, 'ifDescription', (sampler_ip, in_if), concat(sampler_ip, '-', in_if)),

`out_if_name` String ALIAS dictGetOrDefault(default.engt_ifaces_dict, 'ifDescription', (sampler_ip, out_if), concat(sampler_ip, '-', out_if)),

`etype_name` String ALIAS dictGetOrDefault(default.ethertypes_dict, 'Keyword', etype, etype),
`proto_name` String ALIAS dictGetOrDefault(default.iana_protocols_dict, 'Keyword', proto, proto),
`src_mac_name` String ALIAS MACNumToString(src_mac),
`dst_mac_name` String ALIAS MACNumToString(dst_mac),
`ip_dscp` UInt32 ALIAS bitShiftRight(ip_tos, 2),
`dir_in` Bool ALIAS dictHas(default.engt_ifaces_dict, (sampler_ip, in_if)),
`dir_out` Bool ALIAS dictHas(default.engt_ifaces_dict, (sampler_ip, out_if))

Grafana dashboard

Dashboard controls

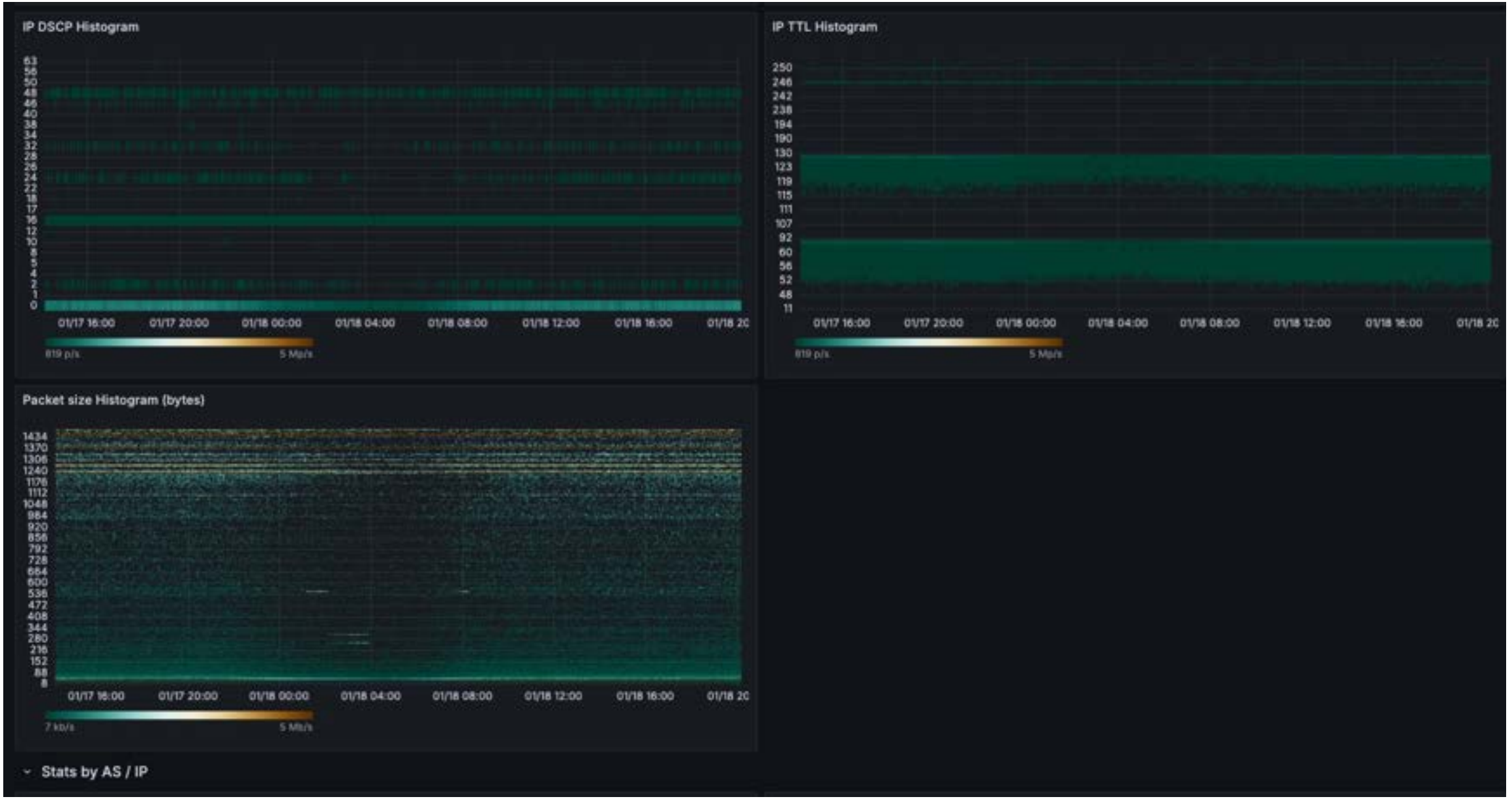


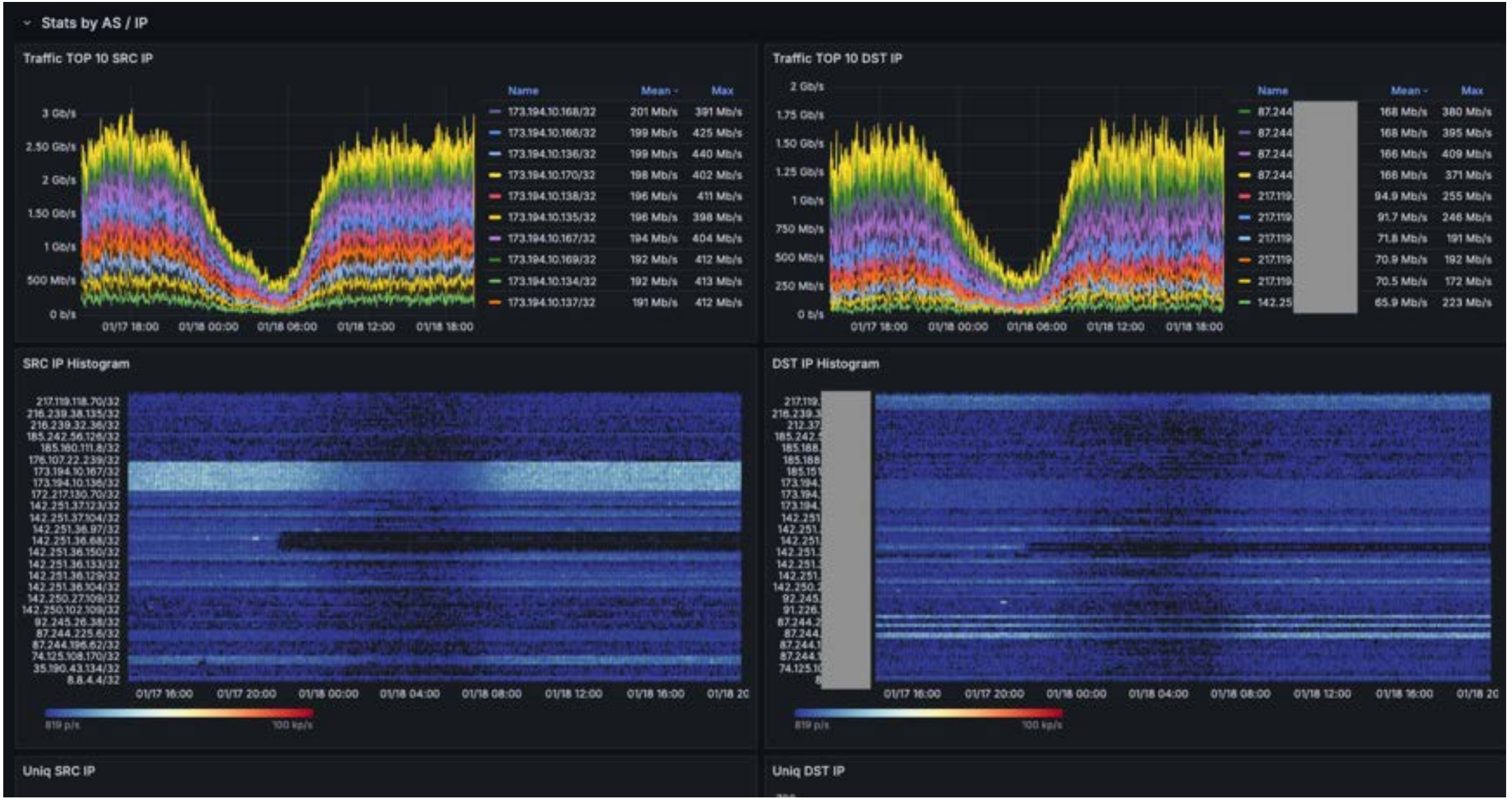
- FILTER – „user frendy“ filter (with autocomplete)
- TTYPE – predefined filters (SYN only, fragments, UDP 53/161, …)
- QUERY – custom SQL filter statements (not colleague friendly but my favorite)
- SAMPLING – static or dynamic sampling rate when generating graphs (dynamic adjusts by actual time window - shorter the window, lower the sampling rate till 1/1)
- AGGR_IPv4 / AGGR_IPv6 – cumulate data by specified IP range
- TOP_N – how many TOP N items to render in graphs in whole dashboard

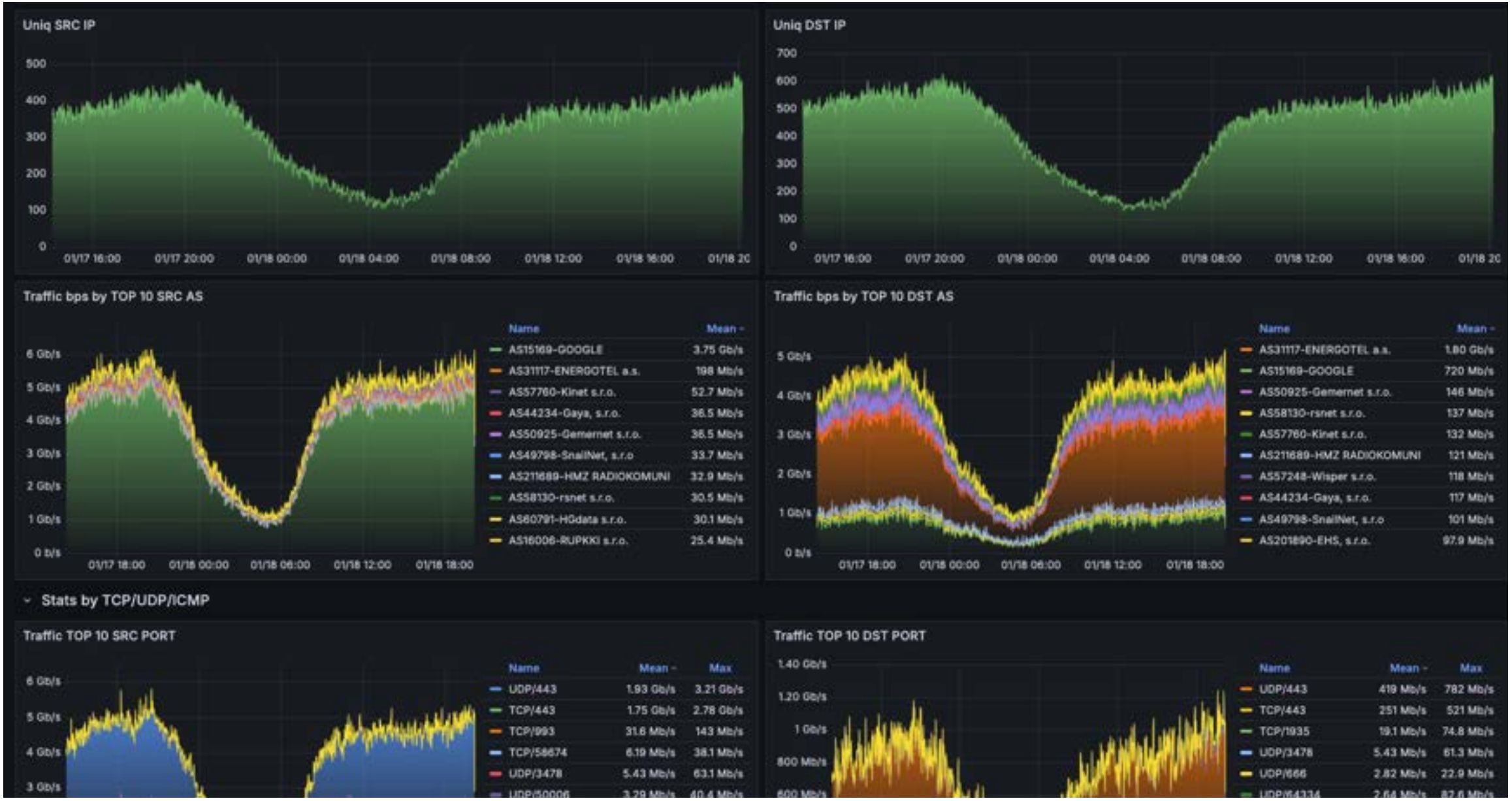

Home › Dashboards › Clickhouse
Share
Edit
FILTER
TTYPE OBFUSCATED
QUERY src_as=15169 or dst_as=15169
SAMPLING low dynamic
AGGR_IPv4 32
AGGR_IPv6 128
TOP_N 10
Last 30 hours
Refresh
Overall traffic
8 Gb/s
7 Gb/s
6 Gb/s
5 Gb/s
4 Gb/s
3 Gb/s
2 Gb/s
1 Gb/s
0 b/s
-1 Gb/s
-2 Gb/s
-3 Gb/s
-4 Gb/s
-5 Gb/s
-6 Gb/s
-7 Gb/s
-8 Gb/s
800 kp/s
700 kp/s
600 kp/s
500 kp/s
400 kp/s
300 kp/s
200 kp/s
100 kp/s
0 p/s
-100 kp/s
-200 kp/s
-300 kp/s
-400 kp/s
-500 kp/s
-600 kp/s
-700 kp/s
-800 kp/s
01/17 15:00
01/17 18:00
01/17 21:00
01/18 00:00
01/18 03:00
01/18 06:00
01/18 09:00
01/18 12:00
01/18 15:00
01/18 18:00
Name Mean Max Last
bitsIn 3.76 Gb/s 5.89 Gb/s 3.04 Gb/s
bitsOut -722 Mb/s 0 b/s -909 Mb/s
pktsIn (right y-axis) 428 kp/s 660 kp/s 358 kp/s
pktsOut (right y-axis) -184 kp/s 0 p/s -199 kp/s
Stats by IN / OUT Interface
Traffic bps by interface
6 Gb/s
5 Gb/s
Name Mean Max Last
NIX.SK IN 1.54 Gb/s 2.38 Gb/s 2.34 Gb/s
NIX.CZ IN 1.53 Gb/s 2.37 Gb/s 1.92 Gb/s
PEERING.CZ IN 667 Mb/s 1.18 Gb/s 951 Mb/s

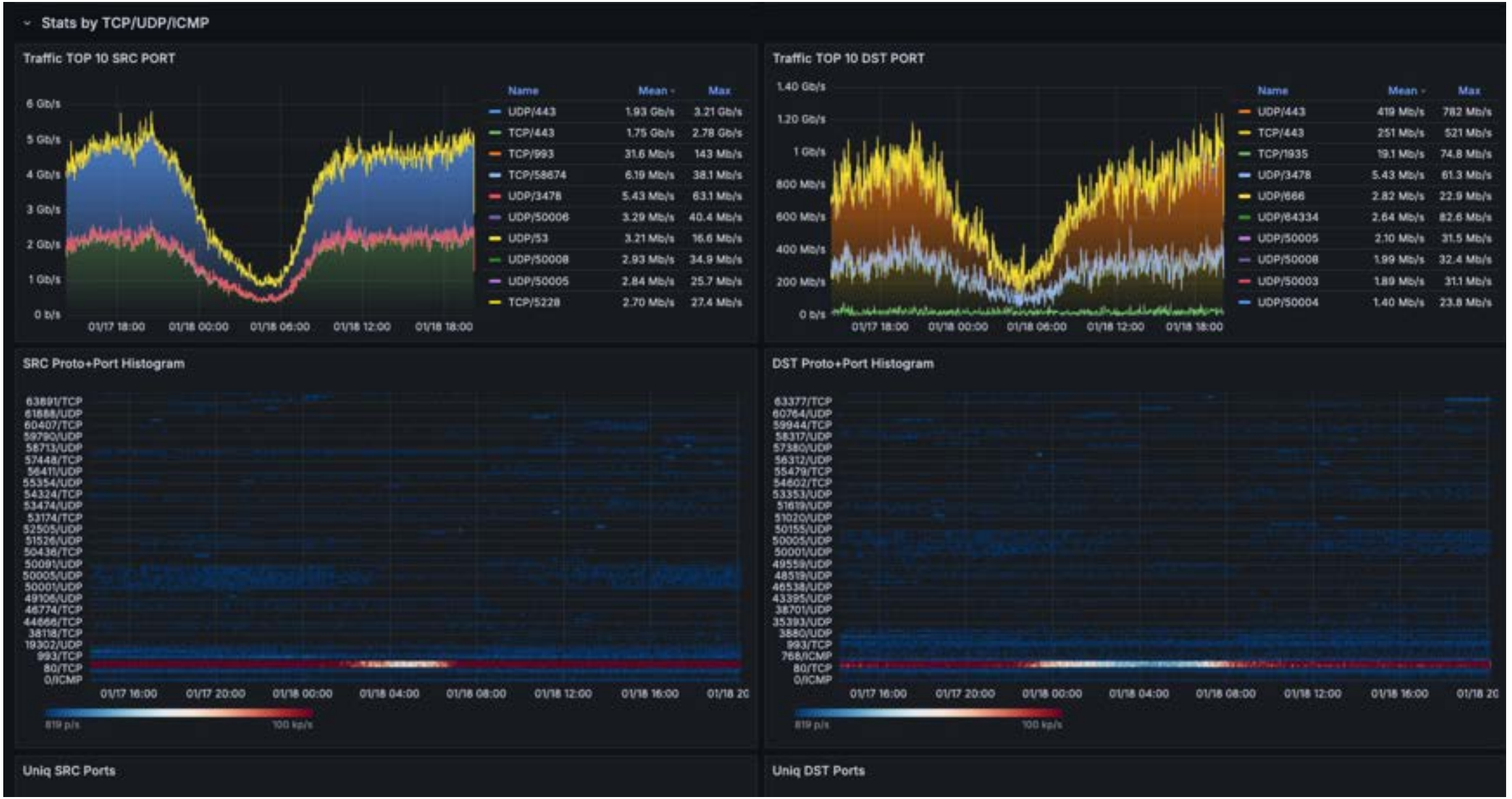

Stats by IN / OUT Interface
Traffic bps by Interface
6 Gb/s
5 Gb/s
4 Gb/s
3 Gb/s
2 Gb/s
1 Gb/s
0 b/s
-1 Gb/s
-2 Gb/s
01/17 16:00
01/17 18:00
01/17 20:00
01/17 22:00
01/18 00:00
01/18 02:00
01/18 04:00
01/18 06:00
01/18 08:00
01/18 10:00
01/18 12:00
01/18 14:00
01/18 16:00
01/18 18:00
01/18 20
Name
Mean
Max
Last
NIX.SK IN 1.54 Gb/s 2.38 Gb/s 2.34 Gb/s
NIX.CZ IN 1.53 Gb/s 2.37 Gb/s 1.92 Gb/s
PEERING.CZ IN 667 Mb/s 1.18 Gb/s 951 Mb/s
ORANGE IN 8.87 Mb/s 58.6 Mb/s 31.4 Mb/s
SIX.SK IN 5.28 Mb/s 62.8 Mb/s 262 kb/s
SUPERNET_02 IN 4.99 Mb/s 49.6 Mb/s 655 kb/s
SUPERNET_01 IN 4.75 Mb/s 41.7 Mb/s 0 b/s
SWAN.SK IN 288 kb/s 23.4 Mb/s 0 b/s
SIX2.SK IN 45.5 kb/s 9.52 Mb/s 0 b/s
1-IX IN 1.03 kb/s 465 kb/s 0 b/s
1-IX OUT -237 b/s 0 b/s 0 b/s
SUPERNET_02 OUT -2.54 Mb/s 0 b/s 0 b/s
SWAN.SK OUT -3.17 Mb/s 0 b/s -629 kb/s
SIX2.SK OUT -3.49 Mb/s 0 b/s 0 b/s
ORANGE OUT -13.2 Mb/s 0 b/s -10.4 Mb/s
PEERING.CZ OUT -14.6 Mb/s 0 b/s -25.5 Mb/s
NIX.CZ OUT -686 Mb/s -108 Mb/s -1.08 Gb/s
IP Analysis
EtherTypes TOP 10
IPv4 (0x0800) 98.53%
IPv6 (0x86DD) 1.47%
IP Flags
DONT_FRAGMENT 62.04%
NONE 37.95%
MORE_FRAGMENTS 0.01%
RESERVED_BIT 0.00%
NONE
DONT_FRAGMENT

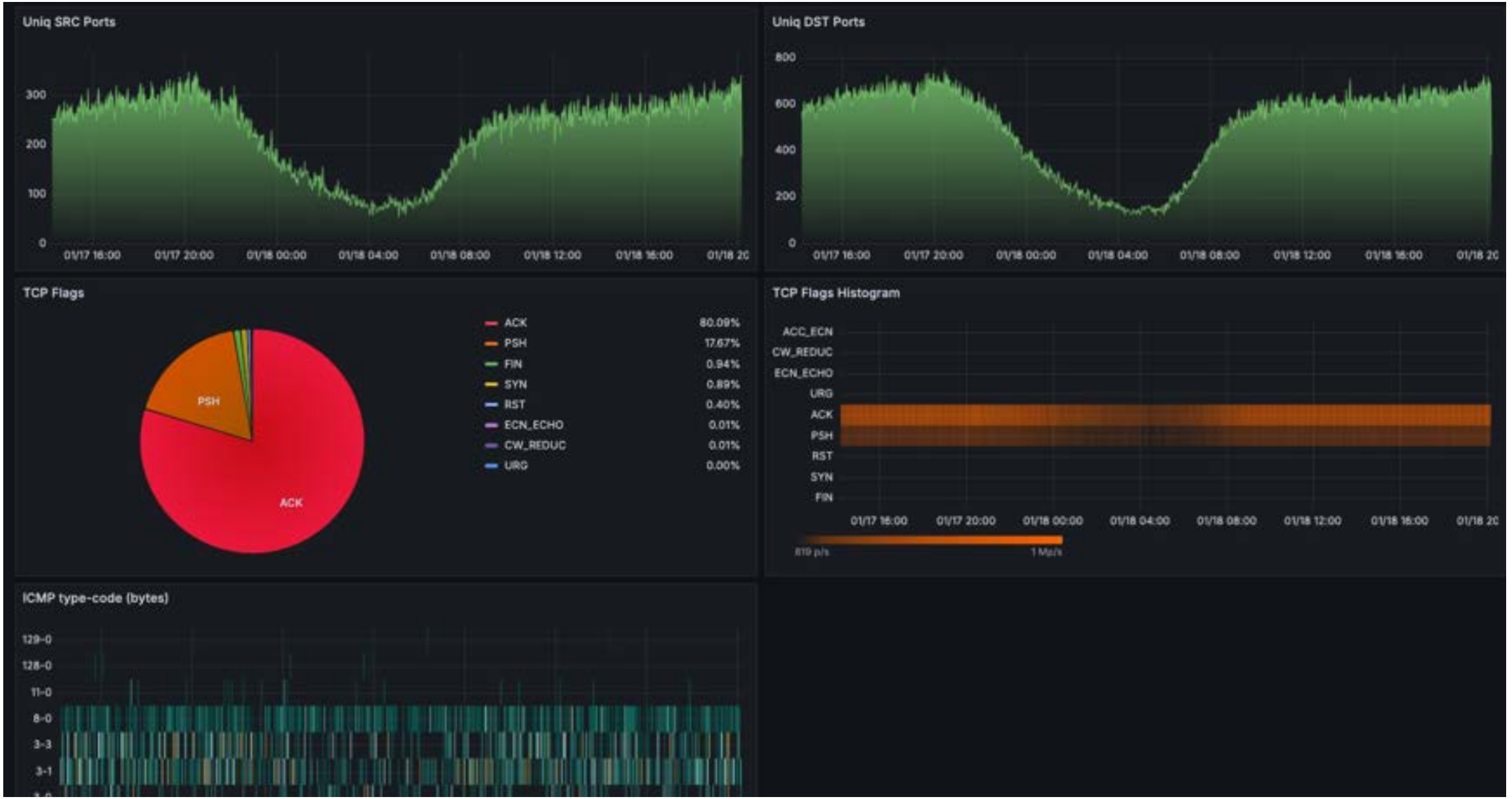

IP Analysis
EtherTypes TOP 10
IPv4 (0x0800) 98.53%
IPv6 (0x86DD) 1.47%
IPv4 (0x0800)
IP Flags
DONT_FRAGMENT 62.04%
NONE 37.95%
MORE_FRAGMENTS 0.01%
RESERVED_BIT 0.00%
NONE
DONT_FRAGMENT
Fragment Offset Histogram
370
368
364
185
184
182
0
01/17 16:00
01/17 20:00
01/18 00:00
01/18 04:00
01/18 08:00
01/18 12:00
01/18 16:00
819 p/s
5 Mp/s
IP Flags Histogram
reserved_bit
dont_fragment
more_fragments
01/17 16:00
01/17 20:00
01/18 00:00
01/18 04:00
01/18 08:00
01/18 12:00
01/18 16:00
98 kp/s
5 Mp/s
IP DSCP Histogram
63
56
50
IP TTL Histogram
250
246


IP DSCP Histogram
63
56
50
48
46
40
38
34
32
28
26
24
22
18
17
16
12
10
8
5
4
2
1
0
01/17 16:00
01/17 20:00
01/18 00:00
01/18 04:00
01/18 08:00
01/18 12:00
01/18 16:00
819 p/s
5 Mp/s
IP TTL Histogram
250
246
242
238
194
190
130
123
119
115
111
107
92
60
56
52
48
11
01/17 16:00
01/17 20:00
01/18 00:00
01/18 04:00
01/18 08:00
01/18 12:00
01/18 16:00
819 p/s
5 Mp/s
Packet size Histogram (bytes)
1434
1370
1306
1240
1176
1112
1048
984
920
856
792
728
664
600
536
472
408
344
280
216
152
88
8
01/17 16:00
01/17 20:00
01/18 00:00
01/18 04:00
01/18 08:00
01/18 12:00
01/18 16:00
7 kb/s
5 Mb/s
Stats by AS / IP

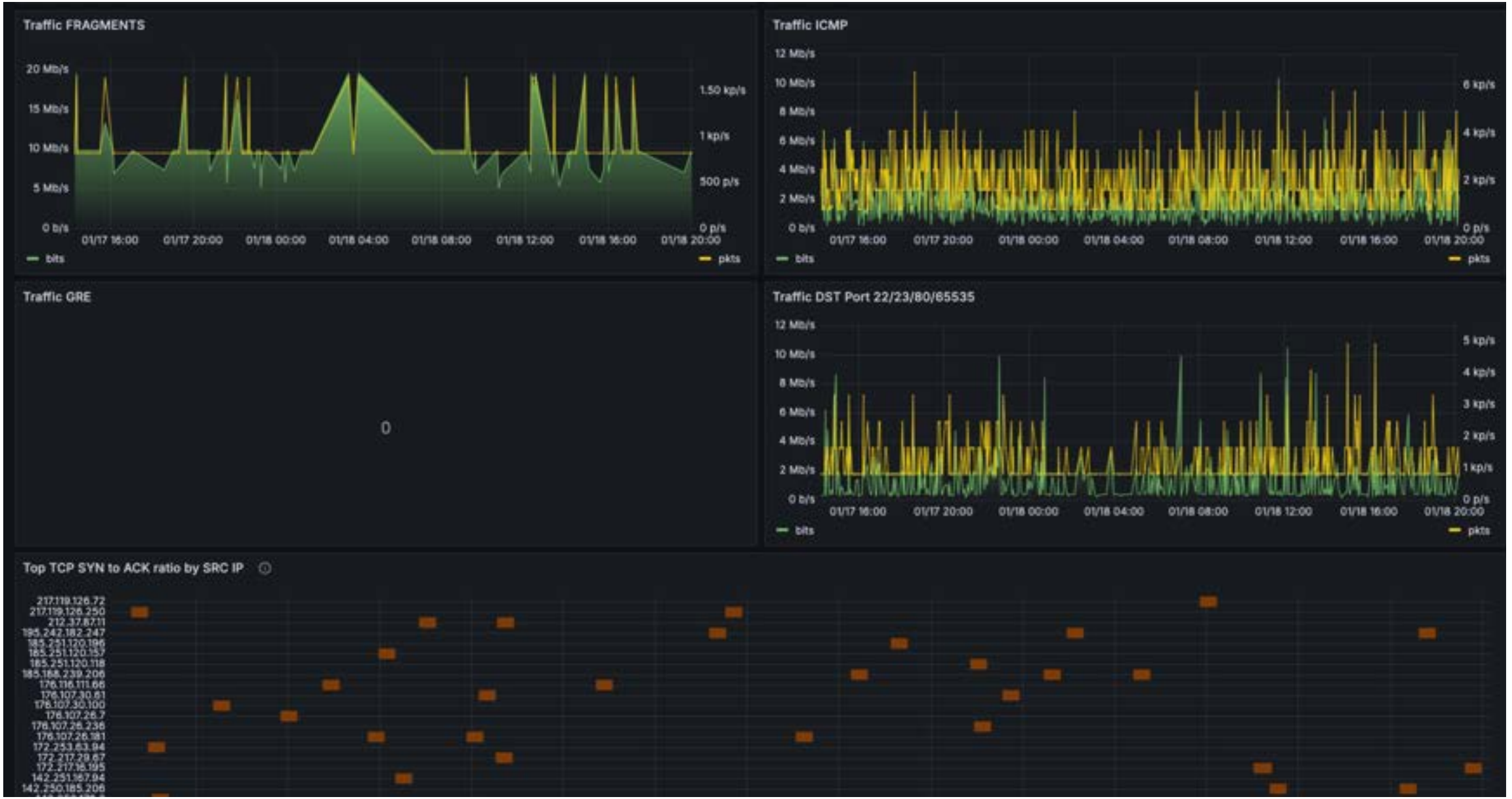

Stats by AS / IP
Traffic TOP 10 SRC IP
Name
Mean
Max
173.194.10.168/32 201 Mb/s 391 Mb/s
173.194.10.166/32 199 Mb/s 425 Mb/s
173.194.10.136/32 199 Mb/s 440 Mb/s
173.194.10.170/32 198 Mb/s 402 Mb/s
173.194.10.138/32 196 Mb/s 411 Mb/s
173.194.10.135/32 196 Mb/s 398 Mb/s
173.194.10.167/32 194 Mb/s 404 Mb/s
173.194.10.169/32 192 Mb/s 412 Mb/s
173.194.10.134/32 192 Mb/s 413 Mb/s
173.194.10.137/32 191 Mb/s 412 Mb/s
3 Gb/s
2.50 Gb/s
2 Gb/s
1.50 Gb/s
1 Gb/s
500 Mb/s
0 b/s
01/17 18:00
01/18 00:00
01/18 06:00
01/18 12:00
01/18 18:00
Traffic TOP 10 DST IP
Name
Mean
Max
87.244 168 Mb/s 380 Mb/s
87.244 168 Mb/s 395 Mb/s
87.244 166 Mb/s 409 Mb/s
87.244 168 Mb/s 371 Mb/s
217.119 94.9 Mb/s 255 Mb/s
217.119 91.7 Mb/s 246 Mb/s
217.119 71.8 Mb/s 191 Mb/s
217.119 70.9 Mb/s 192 Mb/s
217.119 70.5 Mb/s 172 Mb/s
142.25 65.9 Mb/s 223 Mb/s
2 Gb/s
1.75 Gb/s
1.50 Gb/s
1.25 Gb/s
1 Gb/s
750 Mb/s
500 Mb/s
250 Mb/s
0 b/s
01/17 18:00
01/18 00:00
01/18 06:00
01/18 12:00
01/18 18:00
SRC IP Histogram
217.119.118.70/32
216.239.38.135/32
216.239.32.36/32
185.242.56.126/32
185.180.111.8/32
176.107.22.239/32
173.194.10.167/32
173.194.10.136/32
172.217.130.70/32
142.251.37.123/32
142.251.37.104/32
142.251.36.97/32
142.251.36.68/32
142.251.36.150/32
142.251.36.133/32
142.251.36.129/32
142.251.36.104/32
142.250.27.109/32
142.250.102.109/32
92.245.26.38/32
87.244.225.6/32
87.244.196.62/32
74.125.108.170/32
35.190.43.134/32
8.8.4.4/32
01/17 16:00
01/17 20:00
01/18 00:00
01/18 04:00
01/18 08:00
01/18 12:00
01/18 16:00
819 p/s
100 kp/s
DST IP Histogram
01/17 16:00
01/17 20:00
01/18 00:00
01/18 04:00
01/18 08:00
01/18 12:00
01/18 16:00
819 p/s
100 kp/s
Uniq SRC IP
Uniq DST IP


Uniq SRC IP
500
400
300
200
100
0
01/17 16:00
01/17 20:00
01/18 00:00
01/18 04:00
01/18 08:00
01/18 12:00
01/18 16:00
Uniq DST IP
700
600
500
400
300
200
100
0
01/17 16:00
01/17 20:00
01/18 00:00
01/18 04:00
01/18 08:00
01/18 12:00
01/18 16:00
Traffic bps by TOP 10 SRC AS
6 Gb/s
5 Gb/s
4 Gb/s
3 Gb/s
2 Gb/s
1 Gb/s
0 b/s
01/17 18:00
01/18 00:00
01/18 06:00
01/18 12:00
01/18 18:00
Name
Mean
AS15169-GOOGLE 3.75 Gb/s
AS31117-ENERGOTEL a.s. 198 Mb/s
AS57760-Kinet s.r.o. 52.7 Mb/s
AS44234-Gaya, s.r.o. 36.5 Mb/s
AS50925-Gemernet s.r.o. 36.5 Mb/s
AS49798-SnailNet, s.r.o 33.7 Mb/s
AS211689-HMZ RADIOKOMUNI 32.9 Mb/s
AS58130-rsnet s.r.o. 30.5 Mb/s
AS60791-HGdata s.r.o. 30.1 Mb/s
AS16006-RUPKKI s.r.o. 25.4 Mb/s
Traffic bps by TOP 10 DST AS
5 Gb/s
4 Gb/s
3 Gb/s
2 Gb/s
1 Gb/s
0 b/s
01/17 18:00
01/18 00:00
01/18 06:00
01/18 12:00
01/18 18:00
Name
Mean
AS31117-ENERGOTEL a.s. 1.80 Gb/s
AS15169-GOOGLE 720 Mb/s
AS50925-Gemernet s.r.o. 146 Mb/s
AS58130-rsnet s.r.o. 137 Mb/s
AS57760-Kinet s.r.o. 132 Mb/s
AS211689-HMZ RADIOKOMUNI 121 Mb/s
AS57248-Wisper s.r.o. 118 Mb/s
AS44234-Gaya, s.r.o. 117 Mb/s
AS49798-SnailNet, s.r.o 101 Mb/s
AS201890-EHS, s.r.o. 97.9 Mb/s
Stats by TCP/UDP/ICMP
Traffic TOP 10 SRC PORT
6 Gb/s
5 Gb/s
4 Gb/s
3 Gb/s
Name
Mean
Max
UDP/443 1.93 Gb/s 3.21 Gb/s
TCP/443 1.75 Gb/s 2.78 Gb/s
TCP/993 31.6 Mb/s 143 Mb/s
TCP/58674 6.19 Mb/s 38.1 Mb/s
UDP/3478 5.43 Mb/s 63.1 Mb/s
Traffic TOP 10 DST PORT
1.40 Gb/s
1.20 Gb/s
1 Gb/s
800 Mb/s
Name
Mean
Max
UDP/443 419 Mb/s 782 Mb/s
TCP/443 251 Mb/s 521 Mb/s
TCP/1935 19.1 Mb/s 74.8 Mb/s
UDP/3478 5.43 Mb/s 61.3 Mb/s
UDP/666 2.82 Mb/s 22.9 Mb/s


Stats by TCP/UDP/ICMP
Traffic TOP 10 SRC PORT
6 Gb/s
5 Gb/s
4 Gb/s
3 Gb/s
2 Gb/s
1 Gb/s
0 b/s
01/17 18:00
01/18 00:00
01/18 06:00
01/18 12:00
01/18 18:00
Name Mean Max
UDP/443 1.93 Gb/s 3.21 Gb/s
TCP/443 1.75 Gb/s 2.78 Gb/s
TCP/993 31.6 Mb/s 143 Mb/s
TCP/58674 6.19 Mb/s 38.1 Mb/s
UDP/3478 5.43 Mb/s 63.1 Mb/s
UDP/50006 3.29 Mb/s 40.4 Mb/s
UDP/53 3.21 Mb/s 16.6 Mb/s
UDP/50008 2.93 Mb/s 34.9 Mb/s
UDP/50005 2.84 Mb/s 25.7 Mb/s
TCP/5228 2.70 Mb/s 27.4 Mb/s
Traffic TOP 10 DST PORT
1.40 Gb/s
1.20 Gb/s
1 Gb/s
800 Mb/s
600 Mb/s
400 Mb/s
200 Mb/s
0 b/s
01/17 18:00
01/18 00:00
01/18 06:00
01/18 12:00
01/18 18:00
Name Mean Max
UDP/443 419 Mb/s 782 Mb/s
TCP/443 251 Mb/s 521 Mb/s
TCP/1935 19.1 Mb/s 74.8 Mb/s
UDP/3478 5.43 Mb/s 61.3 Mb/s
UDP/666 2.82 Mb/s 22.9 Mb/s
UDP/64334 2.64 Mb/s 82.6 Mb/s
UDP/50005 2.10 Mb/s 31.5 Mb/s
UDP/50008 1.99 Mb/s 32.4 Mb/s
UDP/50003 1.89 Mb/s 31.1 Mb/s
UDP/50004 1.40 Mb/s 23.8 Mb/s
SRC Proto+Port Histogram
63891/TCP
61888/UDP
60407/TCP
59790/UDP
58713/UDP
57448/TCP
56411/UDP
55354/UDP
54324/TCP
53474/UDP
53174/TCP
52505/UDP
51526/UDP
50436/TCP
50091/UDP
50005/UDP
50001/UDP
49106/UDP
46774/TCP
44666/TCP
38118/TCP
19302/UDP
993/TCP
80/TCP
0/ICMP
01/17 16:00
01/17 20:00
01/18 00:00
01/18 04:00
01/18 08:00
01/18 12:00
01/18 16:00
819 p/s
100 kp/s
DST Proto+Port Histogram
63377/TCP
60764/UDP
59944/TCP
58317/UDP
57380/UDP
56312/UDP
55479/TCP
54602/TCP
53353/UDP
51619/UDP
51020/UDP
50155/UDP
50005/UDP
50001/UDP
49559/UDP
48519/UDP
46538/UDP
43395/UDP
38701/UDP
35393/UDP
3880/UDP
993/TCP
768/ICMP
80/TCP
0/ICMP
01/17 16:00
01/17 20:00
01/18 00:00
01/18 04:00
01/18 08:00
01/18 12:00
01/18 16:00
819 p/s
100 kp/s
Uniq SRC Ports
Uniq DST Ports


Uniq SRC Ports
300
200
100
0
01/17 16:00
01/17 20:00
01/18 00:00
01/18 04:00
01/18 08:00
01/18 12:00
01/18 16:00
Uniq DST Ports
800
600
400
200
0
TCP Flags
PSH
ACK
ACK 80.09%
PSH 17.67%
FIN 0.94%
SYN 0.89%
RST 0.40%
ECN_ECHO 0.01%
CW_REDUC 0.01%
URG 0.00%
TCP Flags Histogram
ACC_ECN
CW_REDUC
ECN_ECHO
URG
ACK
PSH
RST
SYN
FIN
819 p/s
1 Mp/s
ICMP type-code (bytes)
129-0
128-0
11-0
8-0
3-3
3-1

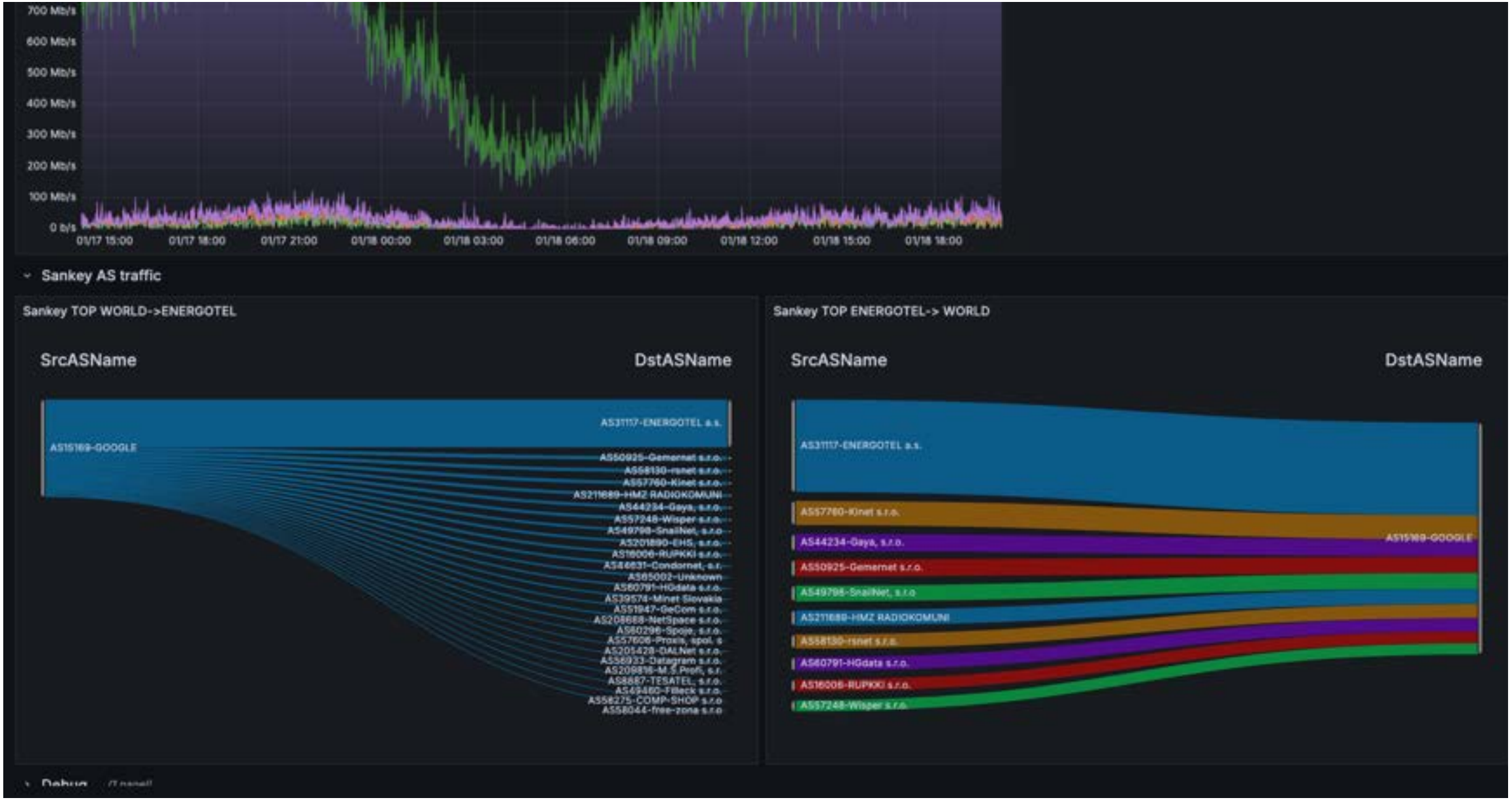

ICMP type-code (bytes)
129-0
128-0
11-0
8-0
3-3
3-1
3-0
1-4
1-3
1-0
0-0
01/17 16:00
01/17 20:00
01/18 00:00
01/18 04:00
01/18 08:00
01/18 12:00
01/18 16:00
52 kb/s
5 Mb/s
Common attack patterns
Traffic SYN only
5 Mb/s
4 Mb/s
3 Mb/s
2 Mb/s
1 Mb/s
0 b/s
6 kp/s
5 kp/s
4 kp/s
3 kp/s
2 kp/s
1 kp/s
0 p/s
01/17 16:00
01/17 20:00
01/18 00:00
01/18 04:00
01/18 08:00
01/18 12:00
01/18 16:00
01/18 20:00
bits
pkts
Traffic SRC Port UDP/53 + UDP/123 + UDP/161 + UDP/11211
20 Mb/s
15 Mb/s
10 Mb/s
5 Mb/s
0 b/s
10 kp/s
8 kp/s
6 kp/s
4 kp/s
2 kp/s
0 p/s
01/17 16:00
01/17 20:00
01/18 00:00
01/18 04:00
01/18 08:00
01/18 12:00
01/18 16:00
01/18 20:00
bits
pkts
Traffic FRAGMENTS
20 Mb/s
Traffic ICMP
12 Mb/s
10 Mb/s
6 kp/s


Traffic FRAGMENTS
20 Mb/s
15 Mb/s
10 Mb/s
5 Mb/s
0 b/s
1.50 kp/s
1 kp/s
500 p/s
0 p/s
01/17 16:00
01/17 20:00
01/18 00:00
01/18 04:00
01/18 08:00
01/18 12:00
01/18 16:00
01/18 20:00
bits
pkts
Traffic ICMP
12 Mb/s
10 Mb/s
8 Mb/s
6 Mb/s
4 Mb/s
2 Mb/s
0 b/s
6 kp/s
4 kp/s
2 kp/s
0 p/s
01/17 16:00
01/17 20:00
01/18 00:00
01/18 04:00
01/18 08:00
01/18 12:00
01/18 16:00
01/18 20:00
bits
pkts
Traffic GRE
0
Traffic DST Port 22/23/80/65535
12 Mb/s
10 Mb/s
8 Mb/s
6 Mb/s
4 Mb/s
2 Mb/s
0 b/s
5 kp/s
4 kp/s
3 kp/s
2 kp/s
1 kp/s
0 p/s
01/17 16:00
01/17 20:00
01/18 00:00
01/18 04:00
01/18 08:00
01/18 12:00
01/18 16:00
01/18 20:00
bits
pkts
Top TCP SYN to ACK ratio by SRC IP
217.119.126.72
217.119.126.250
212.37.87.11
195.242.182.247
185.251.120.196
185.251.120.157
185.251.120.118
185.188.239.206
176.116.111.66
176.107.30.61
176.107.30.100
176.107.26.7
176.107.26.236
176.107.26.181
172.253.63.94
172.217.29.67
172.217.16.195
142.251.167.94
142.250.185.206

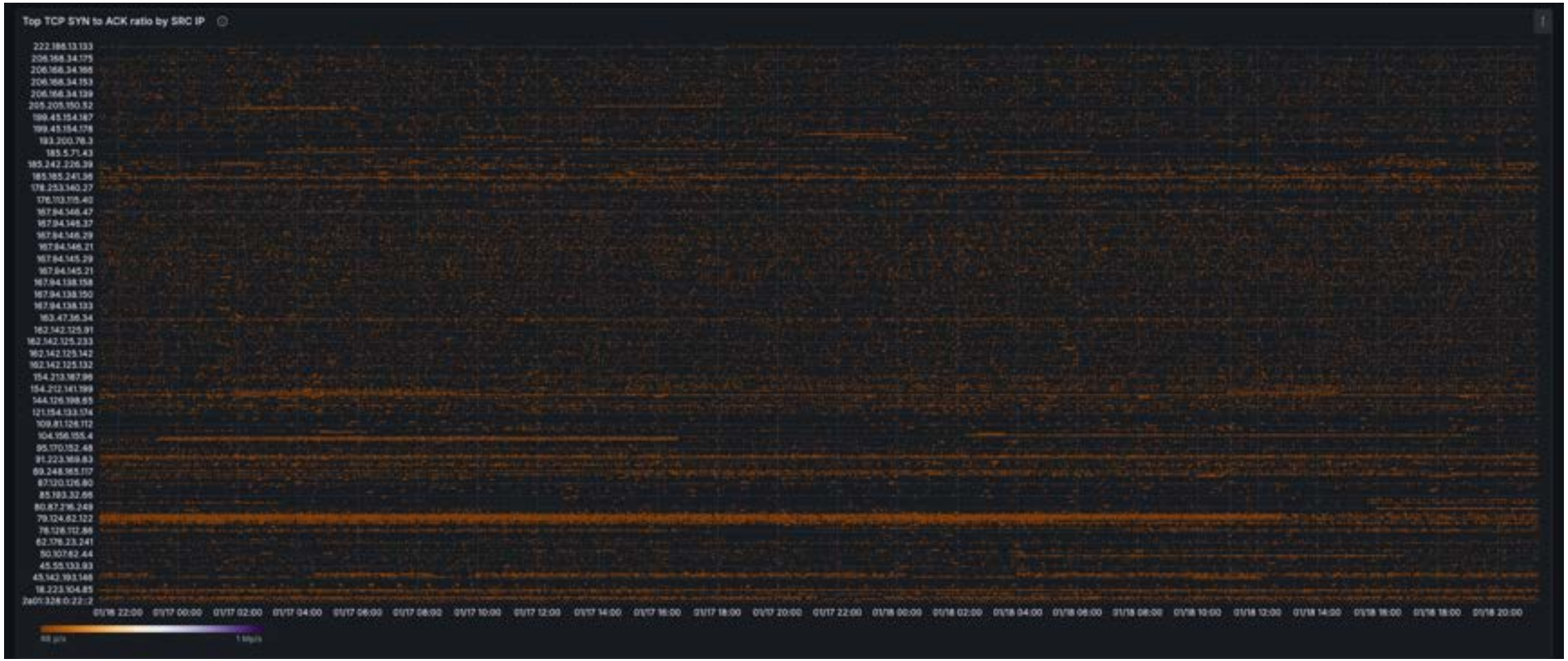

Top TCP SYN to ACK ratio by SRC IP
217.119.126.72
217.119.126.250
212.37.87.11
195.242.182.247
185.251.120.196
185.251.120.157
185.251.120.118
185.188.239.206
176.116.111.66
176.107.30.61
176.107.30.100
176.107.26.7
176.107.26.236
176.107.26.181
172.253.63.94
172.217.29.67
172.217.16.195
142.251.167.94
142.250.185.206
142.250.178.3
142.250.102.108
91.226.114.197
91.226.113.151
91.148.47.12
87.244.235.129
87.244.209.8
87.244.203.8
87.244.195.182
62.169.165.206
46.228.222.25
5.59.168.18
01/17 16:00
01/17 18:00
01/17 20:00
01/17 22:00
01/18 00:00
01/18 02:00
01/18 04:00
01/18 06:00
01/18 08:00
01/18 10:00
01/18 12:00
01/18 14:00
01/18 16:00
01/18 18:00
819 p/s
1 Mp/s
Traffic flow by MAC address (IXP mainly)
Traffic source by SRC MAC (IXP mainly)
6 Gb/s
5.50 Gb/s
5 Gb/s
4.50 Gb/s
4 Gb/s
3.50 Gb/s
3 Gb/s
2.50 Gb/s
Name
Mean
AS15169 - GOOGLE - IX NIX.CZ (00:19:E2:D1:8F:F0) 874 Mb/s
AS15169 - GOOGLE - IX NIX.SK (EC:13:DB:7B:1F:CA) 867 Mb/s
AS15169 - GOOGLE - IX NIX.SK (EC:13:DB:79:89:23) 668 Mb/s
AS15169 - GOOGLE - IX PEERING.CZ (EC:13:DB:79:8F:C8) 666 Mb/s
AS15169 - GOOGLE - IX NIX.CZ (EC:13:DB:79:8F:C3) 653 Mb/s
AS5511 - Orange - TRANZIT ORANGE 9.10 Mb/s
AS39392 - SH.cz s.r.o. - TRANZIT PEERING.CZ 4.94 Mb/s
AS39392 - SH.cz s.r.o. - TRANZIT PEERING.CZ 4.89 Mb/s
AS48326 - DataNetworks s.r. - IX SIX.SK (48:FD:8E:90:FF:71) 3.95 Mb/s
AS6855 - Slovak Telekom, a - IX SIX.SK (F8:39:18:78:E8:17) 1.42 Mb/s


Traffic flow by MAC address (IXP mainly)
Traffic source by SRC MAC (IXP mainly)
6 Gb/s
5.50 Gb/s
5 Gb/s
4.50 Gb/s
4 Gb/s
3.50 Gb/s
3 Gb/s
2.50 Gb/s
2 Gb/s
1.50 Gb/s
1 Gb/s
500 Mb/s
0 b/s
01/17 15:00
01/17 18:00
01/17 21:00
01/18 00:00
01/18 03:00
01/18 06:00
01/18 09:00
01/18 12:00
01/18 15:00
01/18 18:00
Name
Mean
AS15169 - GOOGLE - IX NIX.CZ (00:19:E2:D1:8F:F0) 874 Mb/s
AS15169 - GOOGLE - IX NIX.SK (EC:13:DB:78:1F:CA) 867 Mb/s
AS15169 - GOOGLE - IX NIX.SK (EC:13:DB:79:89:23) 668 Mb/s
AS15169 - GOOGLE - IX PEERING.CZ (EC:13:DB:79:8F:C8) 666 Mb/s
AS15169 - GOOGLE - IX NIX.CZ (EC:13:DB:79:8F:C3) 653 Mb/s
AS5511 - Orange - TRANZIT ORANGE 9.10 Mb/s
AS39392 - SH.cz s.r.o. - TRANZIT PEERING.CZ 4.94 Mb/s
AS39392 - SH.cz s.r.o. - TRANZIT PEERING.CZ 4.89 Mb/s
AS48326 - DataNetworks s.r. - IX SIX.SK (48:FD:8E:90:FF:71) 3.95 Mb/s
AS6855 - Slovak Telekom, a - IX SIX.SK (F8:39:18:78:E8:17) 1.42 Mb/s
Traffic destination by DST MAC (IXP mainly)
1.50 Gb/s
1.40 Gb/s
1.30 Gb/s
1.20 Gb/s
1.10 Gb/s
1 Gb/s
900 Mb/s
800 Mb/s
Name
Mean
AS15169 - GOOGLE - IX NIX.CZ (EC:13:DB:79:8F:C3) 686 Mb/s
AS15169 - GOOGLE - IX PEERING.CZ (EC:13:DB:79:8F:C8) 14.8 Mb/s
AS5511 - Orange - TRANZIT ORANGE 13.2 Mb/s
AS31117 - ENERGOTEL a.s. - TRANZIT ORANGE 8.81 Mb/s
AS48326 - DataNetworks s.r. - IX PEERING.CZ (64:9E:F3:AA:01:FF) 3.85 Mb/s
AS5578 - SWAN, a.s. - TRANZIT SWAN 3.26 Mb/s
AS39392 - SH.cz s.r.o. - TRANZIT PEERING.CZ 2.53 Mb/s
AS24115 - ? - IX 1-IX-EU Equinix WAW (4C:73:4F:28:9B:C0) 233 b/s
AS6939 - HURRICANE - IX NIX.CZ (40:88:2F:BC:28:DD) 160 b/s

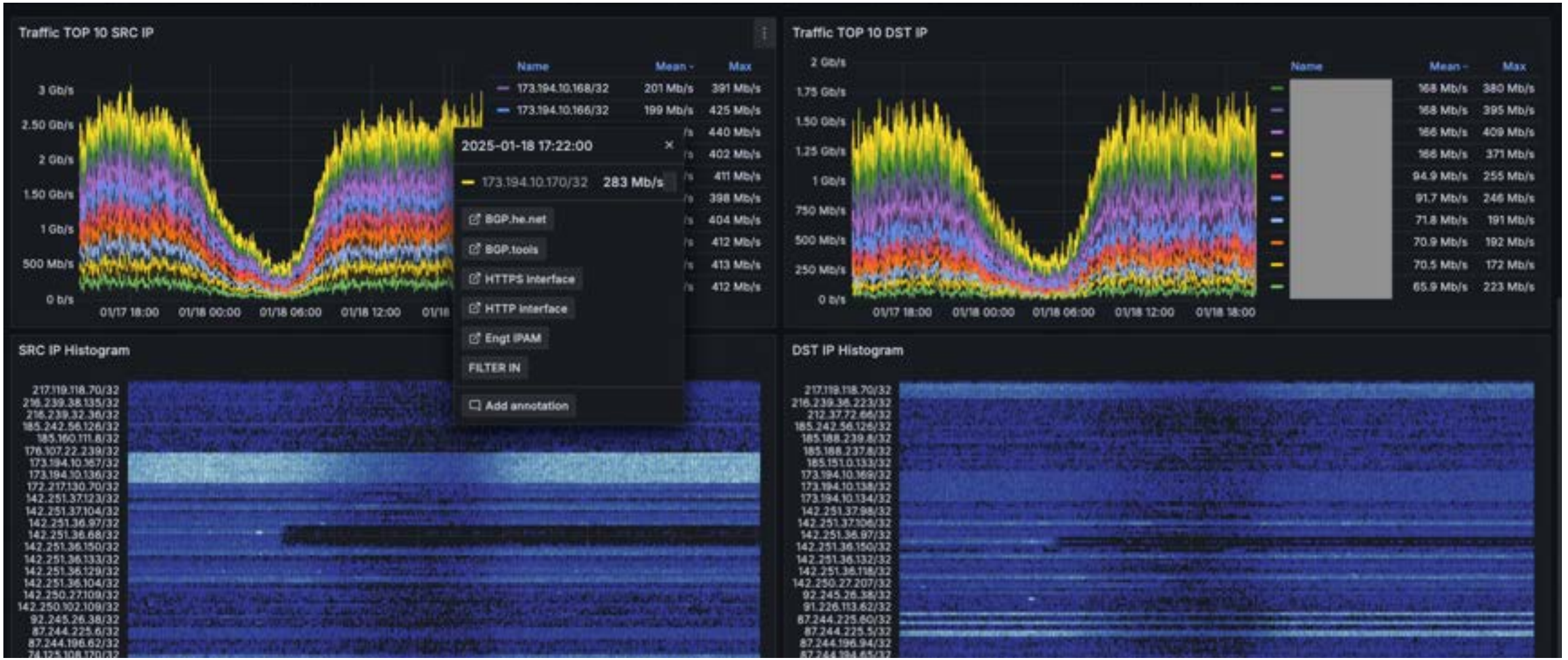

Traffic destination by DST MAC (IXP mainly)
1.50 Gb/s
1.40 Gb/s
1.30 Gb/s
1.20 Gb/s
1.10 Gb/s
1 Gb/s
900 Mb/s
800 Mb/s
700 Mb/s
600 Mb/s
500 Mb/s
400 Mb/s
300 Mb/s
200 Mb/s
100 Mb/s
0 b/s
01/17 15:00
01/17 18:00
01/17 21:00
01/18 00:00
01/18 03:00
01/18 06:00
01/18 09:00
01/18 12:00
01/18 15:00
01/18 18:00
Name
Mean
AS15169 - GOOGLE - IX NIX.CZ (EC:13:D8:79:8F:C3) 686 Mb/s
AS15169 - GOOGLE - IX PEERING.CZ (EC:13:D8:79:8F:C8) 14.8 Mb/s
AS5511 - Orange - TRANZIT ORANGE 13.2 Mb/s
AS31117 - ENERGOTEL a.s. - TRANZIT ORANGE 8.81 Mb/s
AS48326 - DataNetworks s.r. - IX PEERING.CZ (64:9E:F3:AA:01:FF) 3.85 Mb/s
AS5578 - SWAN, a.s. - TRANZIT SWAN 3.26 Mb/s
AS39392 - SH.cz s.r.o. - TRANZIT PEERING.CZ 2.53 Mb/s
AS24115 - ? - IX 1-IX-EU Equinix WAW (4C:73:4F:2B:9B:C0) 233 b/s
AS6939 - HURRICANE - IX NIX.CZ (40:88:2F:8C:28:DD) 160 b/s
Sankey AS traffic
Sankey TOP WORLD->ENERGOTEL
SrcASName
DstASName
AS31117-ENERGOTEL a.s.
AS15169-GOOGLE
AS50925-Gemernet s.r.o.
AS58130-risnet s.r.o.
AS57760-Kinet s.r.o.
AS211689-HMZ RADIOKOMUNI
Sankey TOP ENERGOTEL-> WORLD
SrcASName
DstASName
AS31117-ENERGOTEL a.s.


700 Mb/s
600 Mb/s
500 Mb/s
400 Mb/s
300 Mb/s
200 Mb/s
100 Mb/s
0 b/s
01/17 15:00
01/17 18:00
01/17 21:00
01/18 00:00
01/18 03:00
01/18 06:00
01/18 09:00
01/18 12:00
01/18 15:00
01/18 18:00
Sankey AS traffic
Sankey TOP WORLD->ENERGOTEL
SrcASName
DstASName
AS15169-GOOGLE
AS31117-ENERGOTEL a.s.
AS50925-Gemernet s.r.o.
AS58130-rsnet s.r.o.
AS57760-Kinet s.r.o.
AS211689-HMZ RADIOKOMUNI
AS44234-Gaya, s.r.o.
AS57248-Wisper s.r.o.
AS49798-SnailNet, s.r.o
AS201890-EHS, s.r.o.
AS16006-RUPKKI s.r.o.
AS44631-Condornet, s.r.
AS65002-Unknown
AS60791-HGdata s.r.o.
AS39578-Minet Slovakia
AS51947-GeCom s.r.o.
AS208688-NetSpace s.r.o.
AS60296-Spoje, s.r.o.
AS57606-Proxis, spol. s
AS205428-DALNet s.r.o.
AS56933-Datagram s.r.o.
AS209816-M.S.Profi, s.r.
AS8887-TESATEL, s.r.o.
AS49460-Filleck s.r.o.
AS56275-COMP-SHOP s.r.o
AS58044-free-zona s.r.o
Sankey TOP ENERGOTEL-> WORLD
SrcASName
DstASName
AS31117-ENERGOTEL a.s.
AS57760-Kinet s.r.o.
AS44234-Gaya, s.r.o.
AS50925-Gemernet s.r.o.
AS49798-SnailNet, s.r.o
AS211689-HMZ RADIOKOMUNI
AS58130-rsnet s.r.o.
AS60791-HGdata s.r.o.
AS16006-RUPKKI s.r.o.
AS57248-Wisper s.r.o.
AS15169-GOOGLE

Port scanners detection

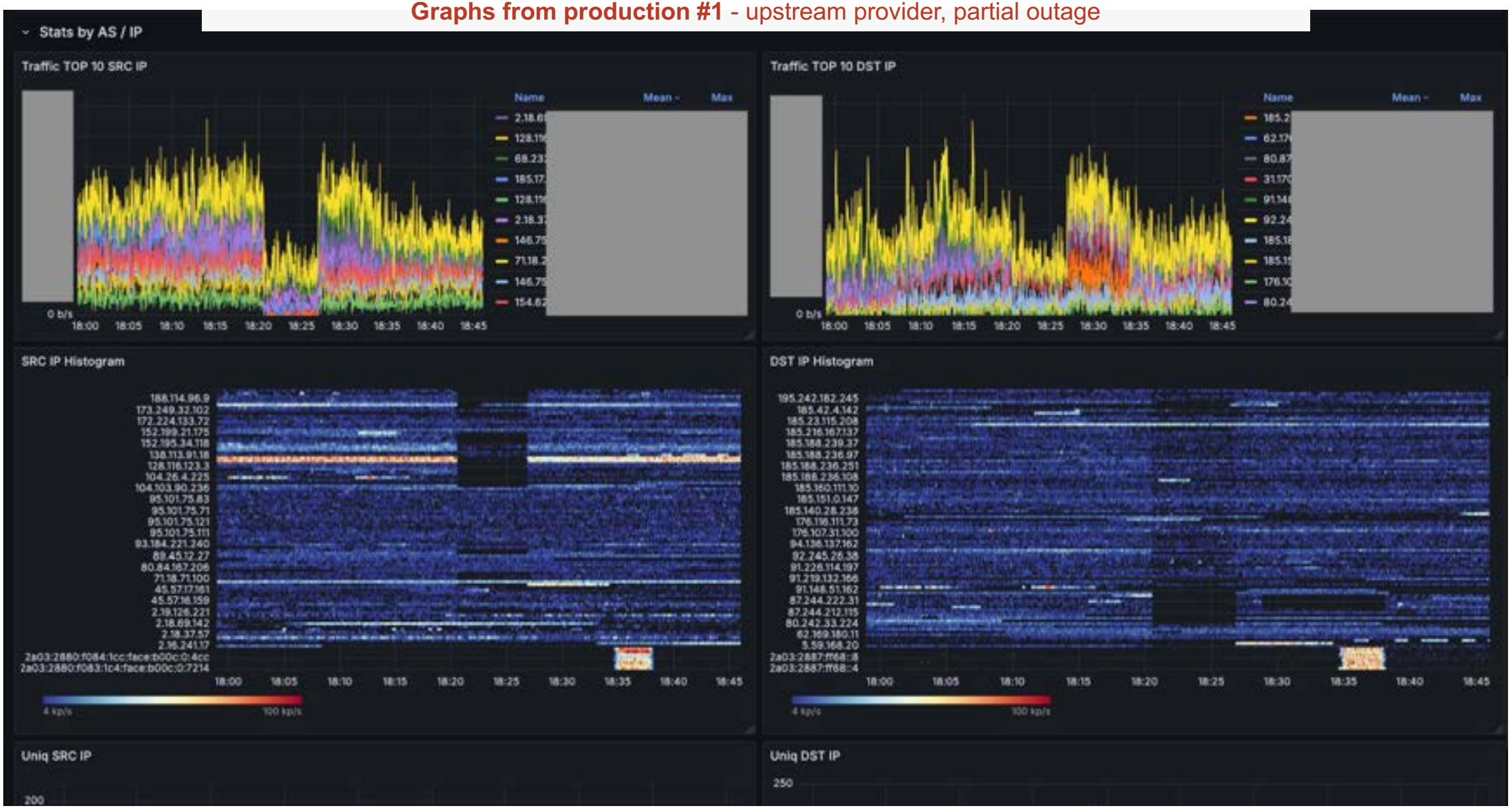


Data links

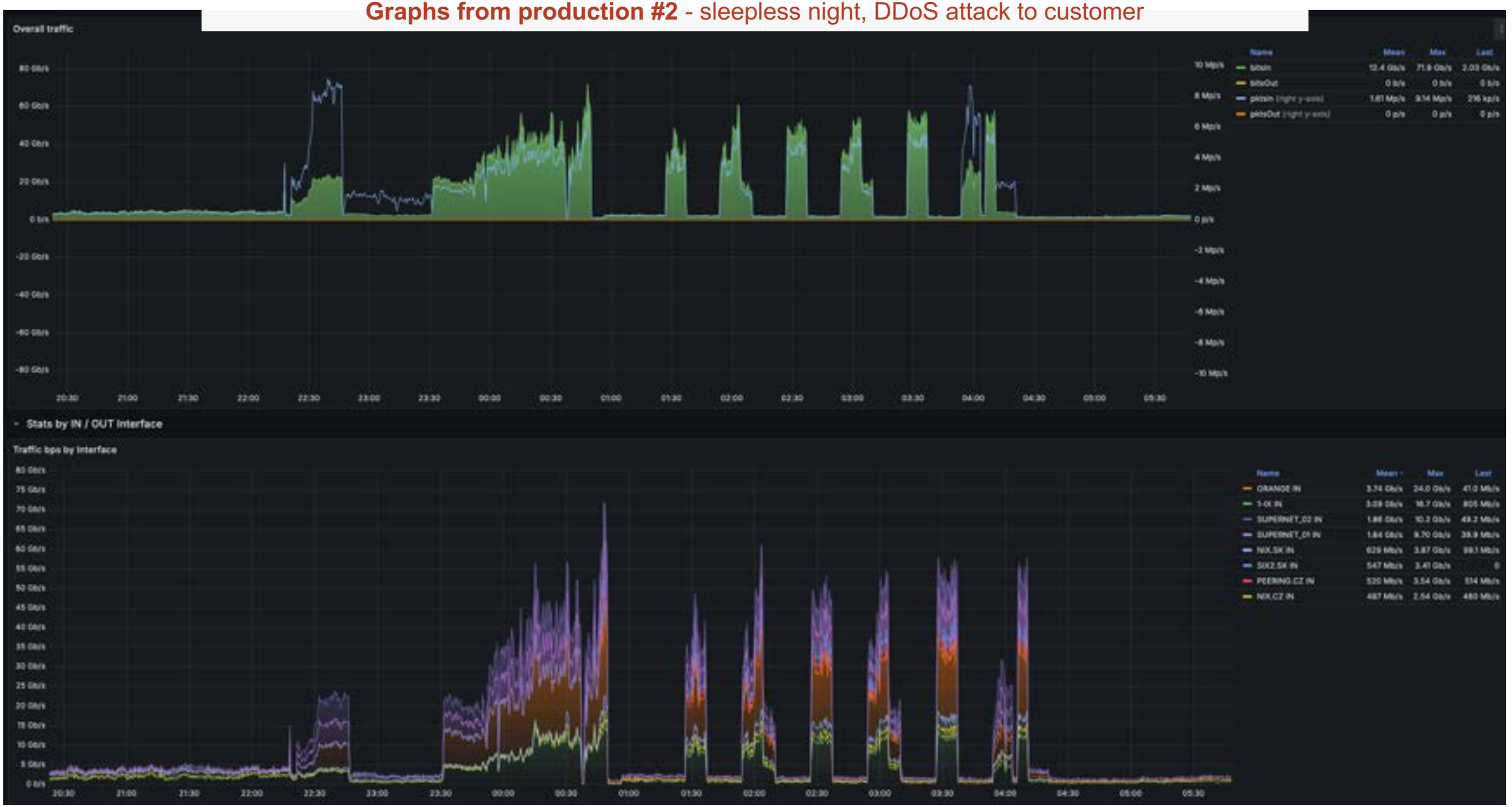

Traffic TOP 10 SRC IP
Name
Mean
Max
173.194.10.168/32 201 Mb/s 391 Mb/s
173.194.10.166/32 199 Mb/s 425 Mb/s
3 Gb/s
2.50 Gb/s
2 Gb/s
1.50 Gb/s
1 Gb/s
500 Mb/s
0 b/s
01/17 18:00
01/18 00:00
01/18 06:00
01/18 12:00
2025-01-18 17:22:00
173.194.10.170/32 283 Mb/s
BGP.he.net
BGP.tools
HTTPS interface
HTTP interface
Engt IPAM
FILTER IN
Add annotation
Traffic TOP 10 DST IP
2 Gb/s
1.75 Gb/s
1.50 Gb/s
1.25 Gb/s
1 Gb/s
750 Mb/s
500 Mb/s
250 Mb/s
0 b/s
01/17 18:00
01/18 00:00
01/18 06:00
01/18 12:00
01/18 18:00
168 Mb/s 380 Mb/s
168 Mb/s 395 Mb/s
166 Mb/s 409 Mb/s
166 Mb/s 371 Mb/s
94.9 Mb/s 255 Mb/s
91.7 Mb/s 246 Mb/s
71.8 Mb/s 191 Mb/s
70.9 Mb/s 192 Mb/s
70.5 Mb/s 172 Mb/s
65.9 Mb/s 223 Mb/s
SRC IP Histogram
217.119.118.70/32
216.239.38.135/32
216.239.32.36/32
185.242.56.126/32
185.160.111.8/32
176.107.22.239/32
173.194.10.167/32
173.194.10.136/32
172.217.130.70/32
142.251.37.123/32
142.251.37.104/32
142.251.36.97/32
142.251.36.68/32
142.251.36.150/32
142.251.36.133/32
142.251.36.129/32
142.251.36.104/32
142.250.27.109/32
142.250.102.109/32
92.245.26.38/32
87.244.225.6/32
87.244.196.62/32
DST IP Histogram
217.119.118.70/32
216.239.38.223/32
212.37.72.66/32
185.242.56.126/32
185.188.239.8/32
185.188.237.8/32
185.151.0.133/32
173.194.10.169/32
173.194.10.138/32
173.194.10.134/32
142.251.37.98/32
142.251.37.106/32
142.251.36.97/32
142.251.36.150/32
142.251.36.132/32
142.251.36.118/32
142.250.27.207/32
92.245.26.38/32
91.226.113.62/32
87.244.225.60/32
87.244.225.5/32
87.244.196.94/32

Graphs from production

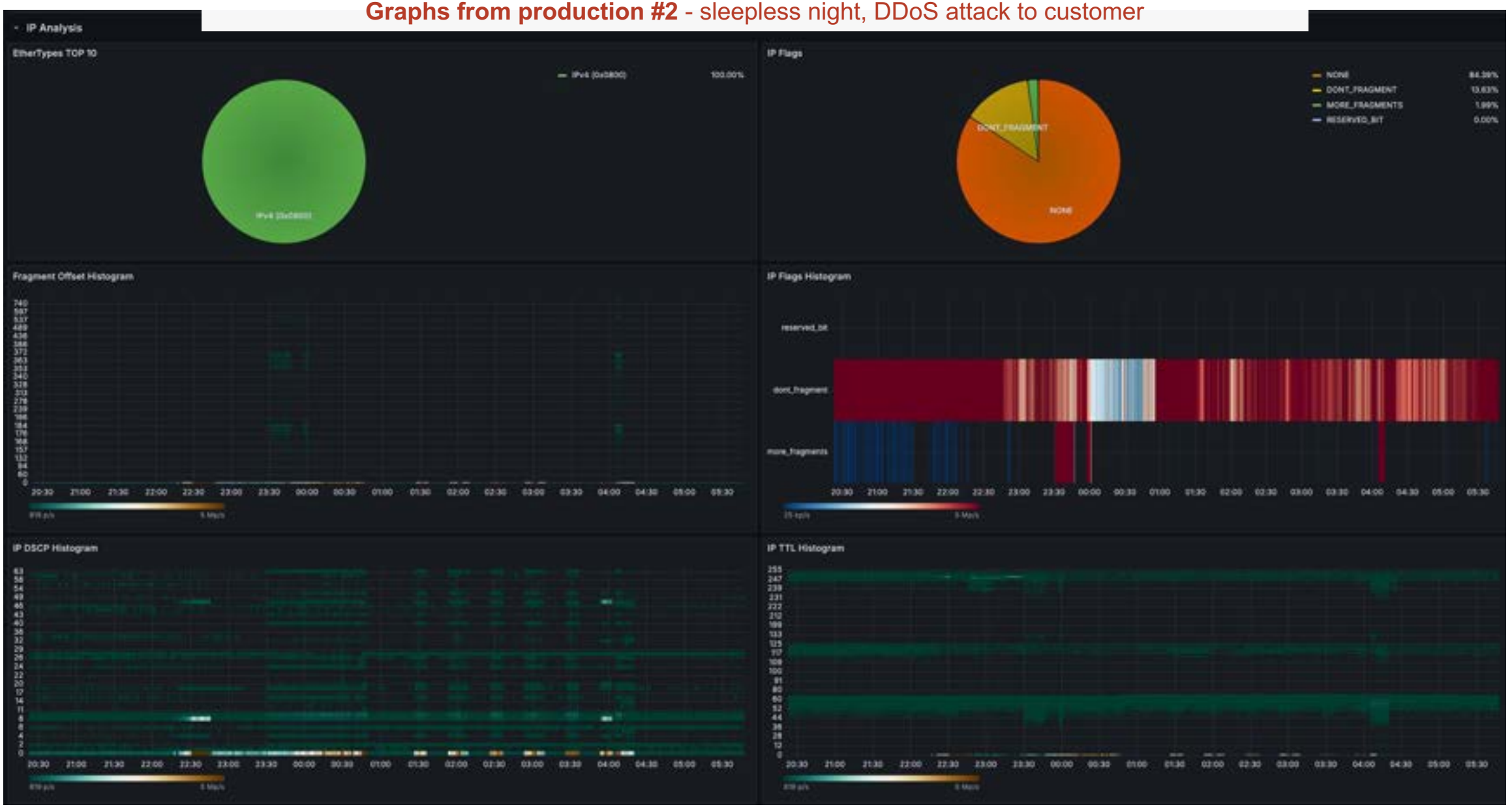
Graphs from production #1 - upstream provider, partial outage



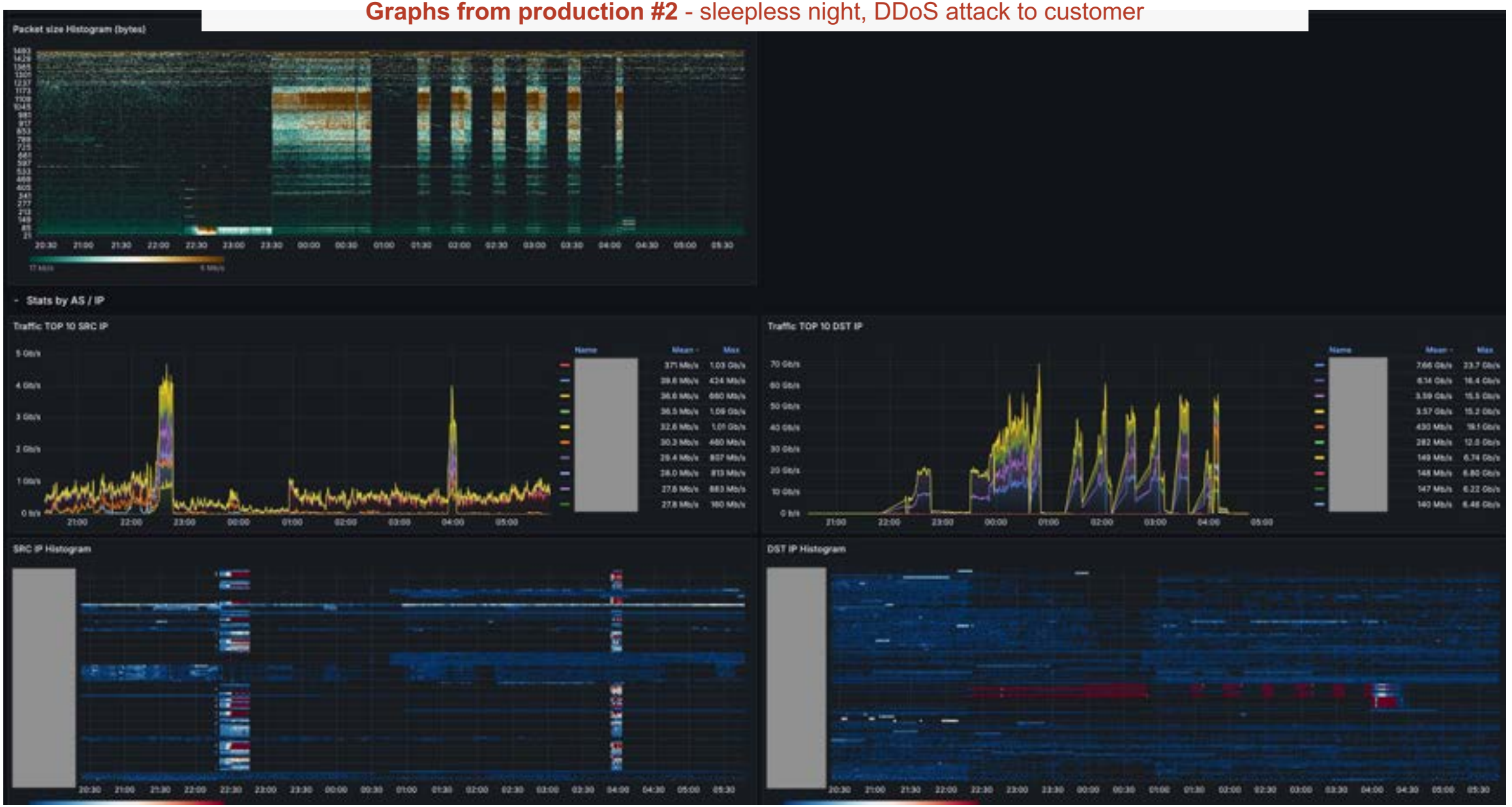
Graphs from production #2 - sleepless night, DDoS attack to customer



Graphs from production #2 - sleepless night, DDoS attack to customer

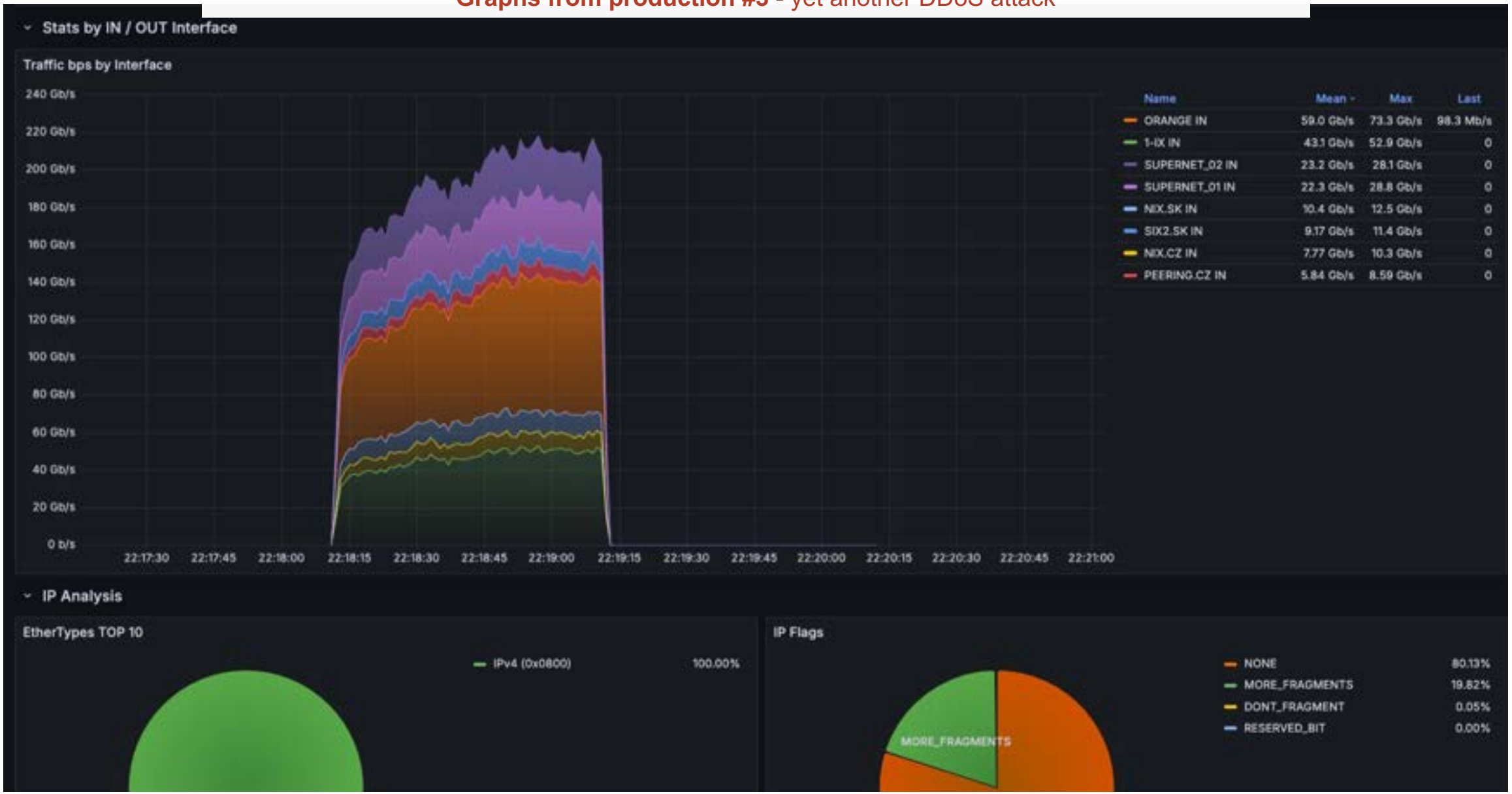


Graphs from production #2 - sleepless night, DDoS attack to customer

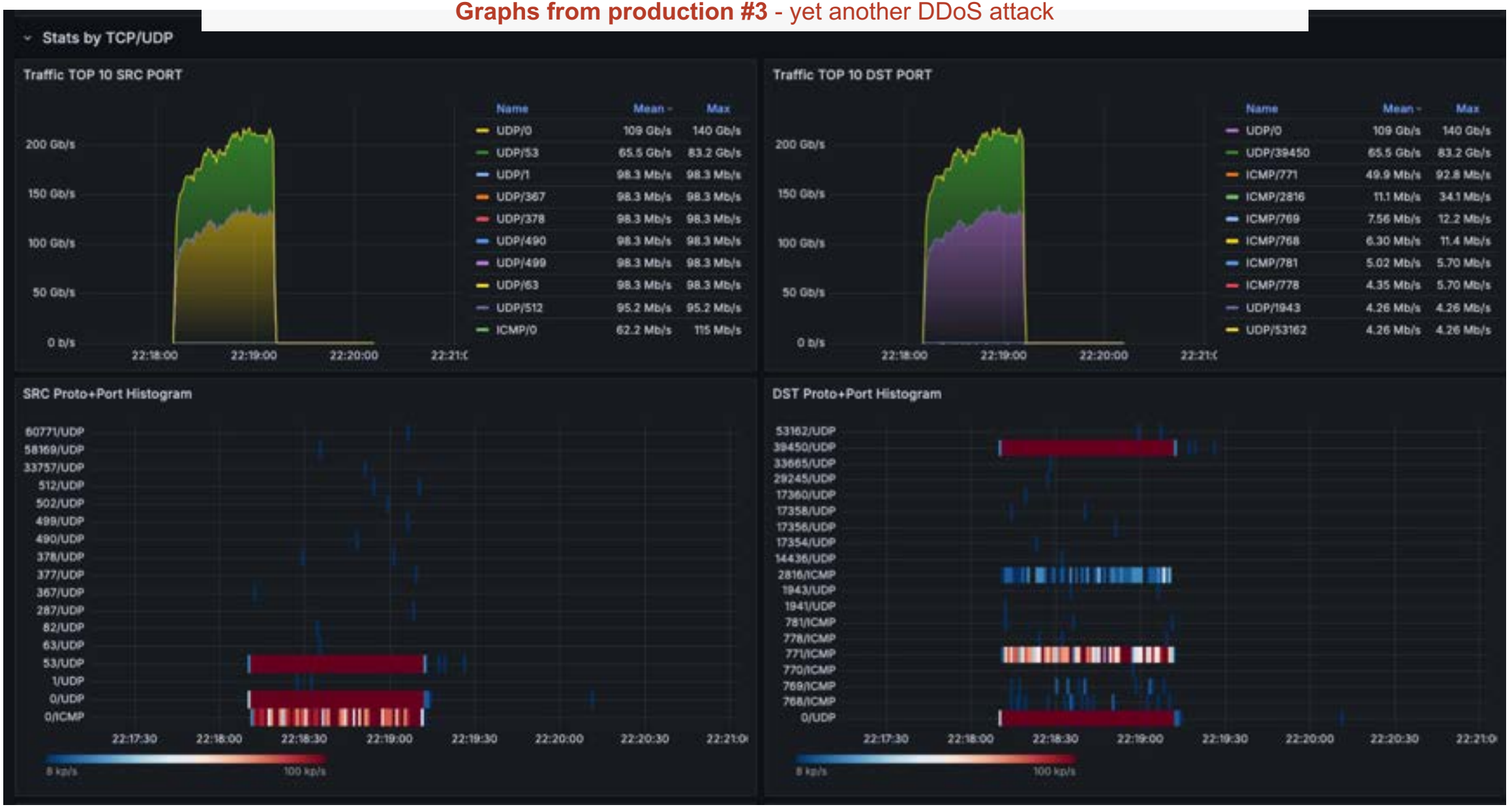


Graphs from production #2 - sleepless night, DDoS attack to customer

Graphs from production #3 - yet another DDoS attack



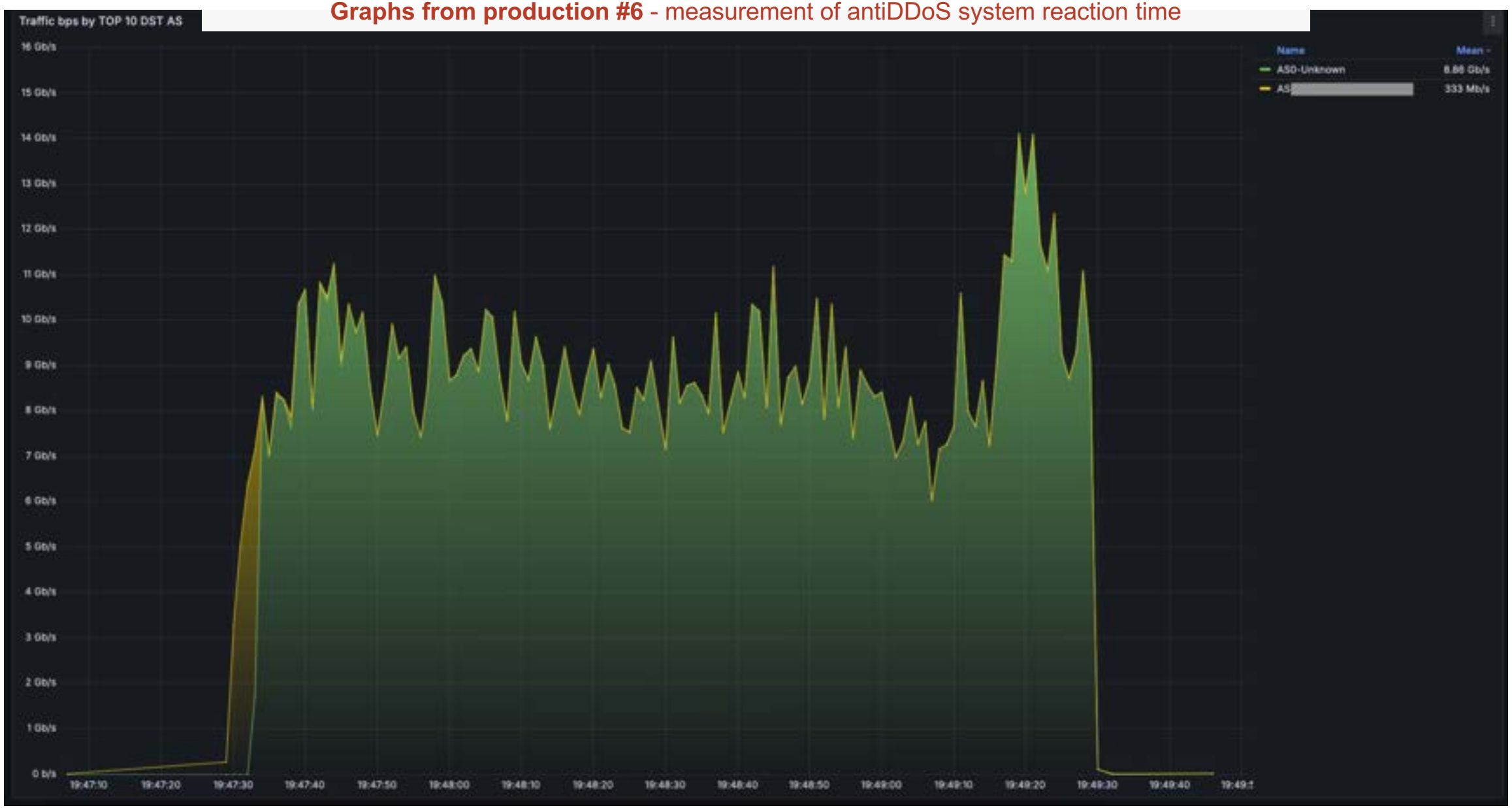
Graphs from production #3 - yet another DDoS attack



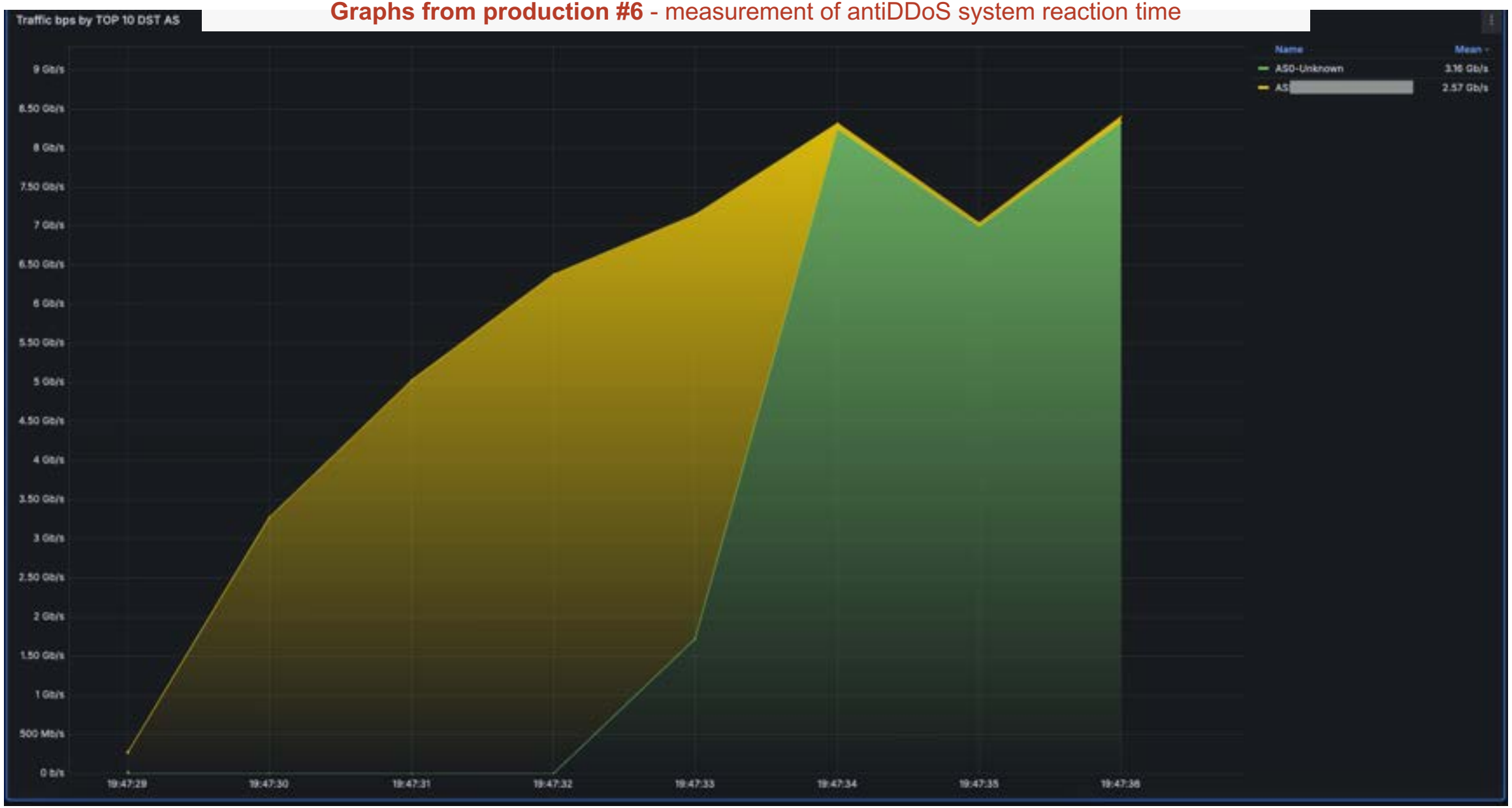
Graphs from production #4 - Fortnite update release, „gamblers look like a stars“

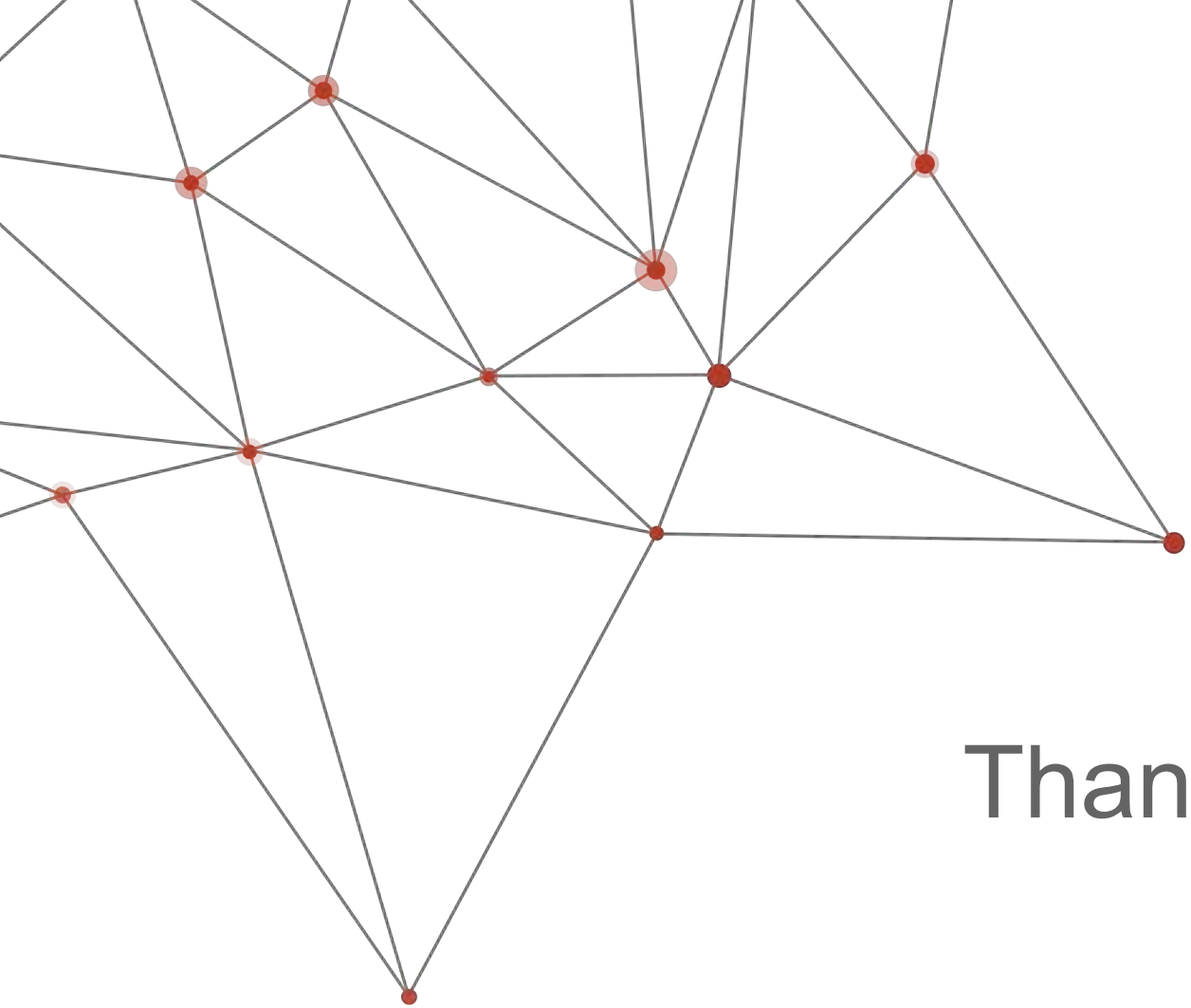
Graphs from production #5 - DDoS attack with destination port sliding each 7 seconds

Graphs from production #6 - measurement of antiDDoS system reaction time



Graphs from production #6 - measurement of antiDDoS system reaction time





Thank you for your attention

Blažej Krajňák

CSNOG | 22.1.2025