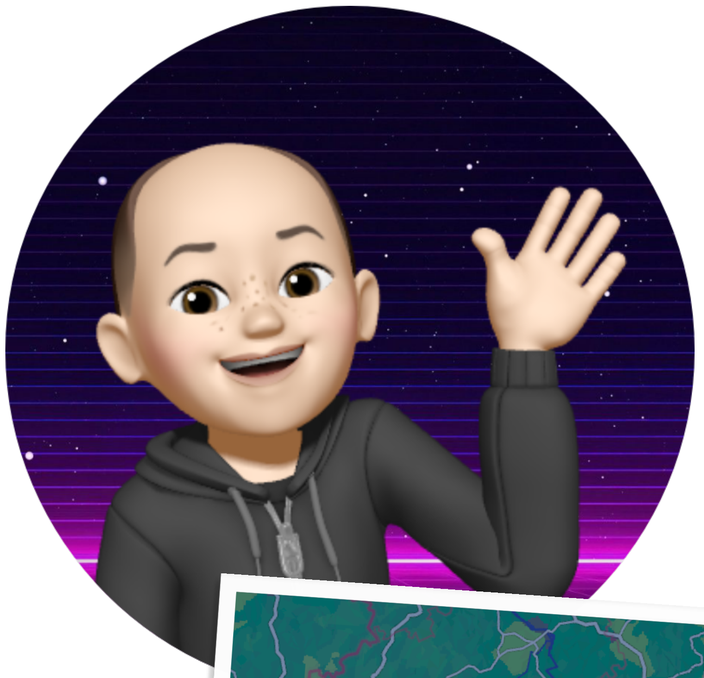
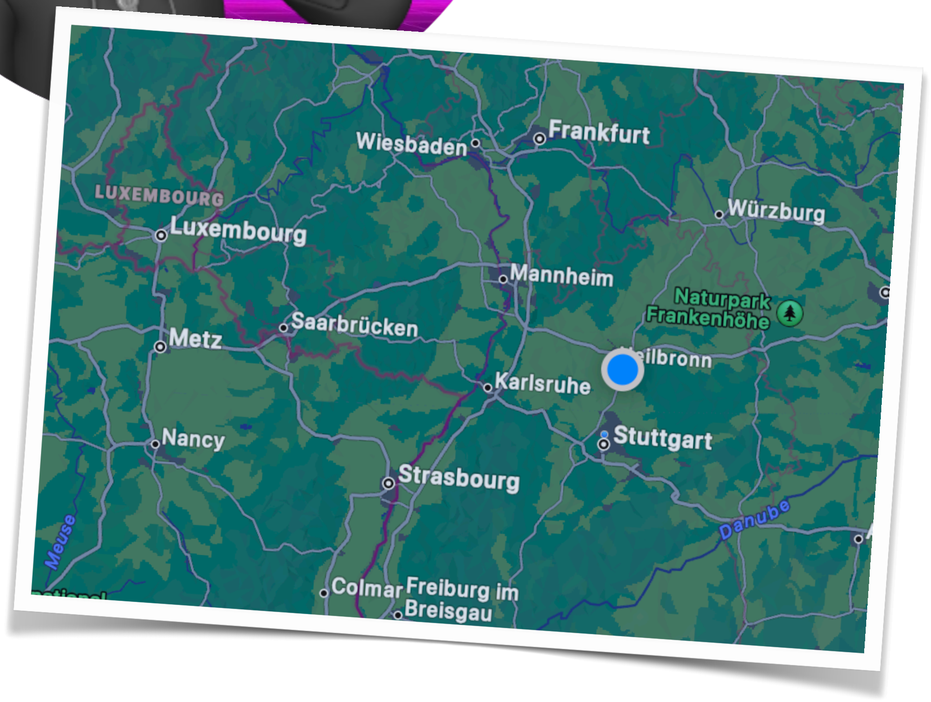
Network Flows

... wo OpenNMS, Nagios überlegen ist.





Ronny Trommer

indigo423 · he/him

I ♥ open source

- Started to use OpenNMS in 2004
- Contributor to OpenNMS since 2008
- Working full-time for OpenNMS since 2015
- openITCOCKPIT Summit 2024

Network Flows

... wo ~~OpenNMS, Nagios~~ überlegen ist.

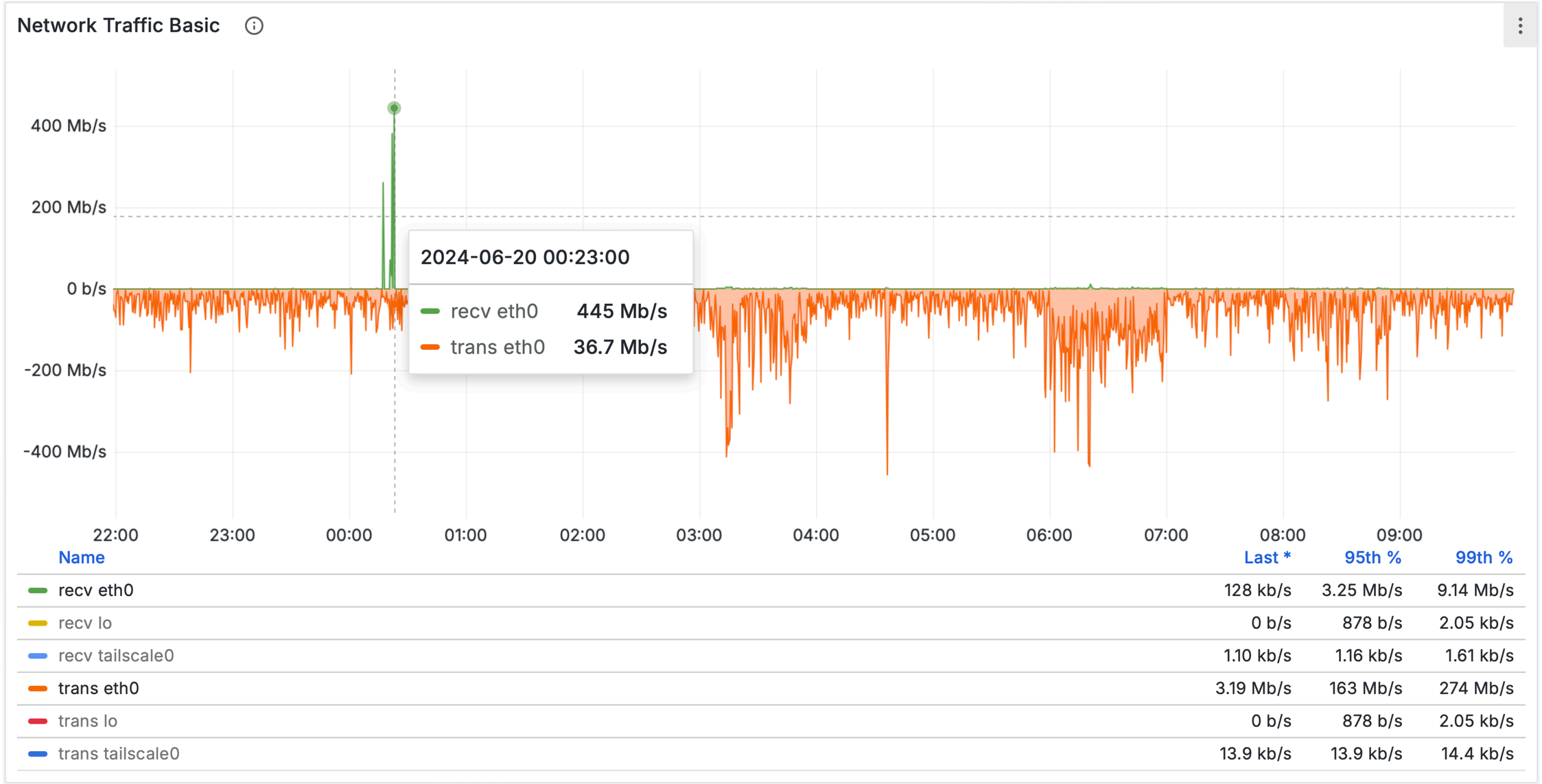
🍎 🥕

Network Flows

... wo ~~OpenNMS, Nagios~~ überlegen ist.

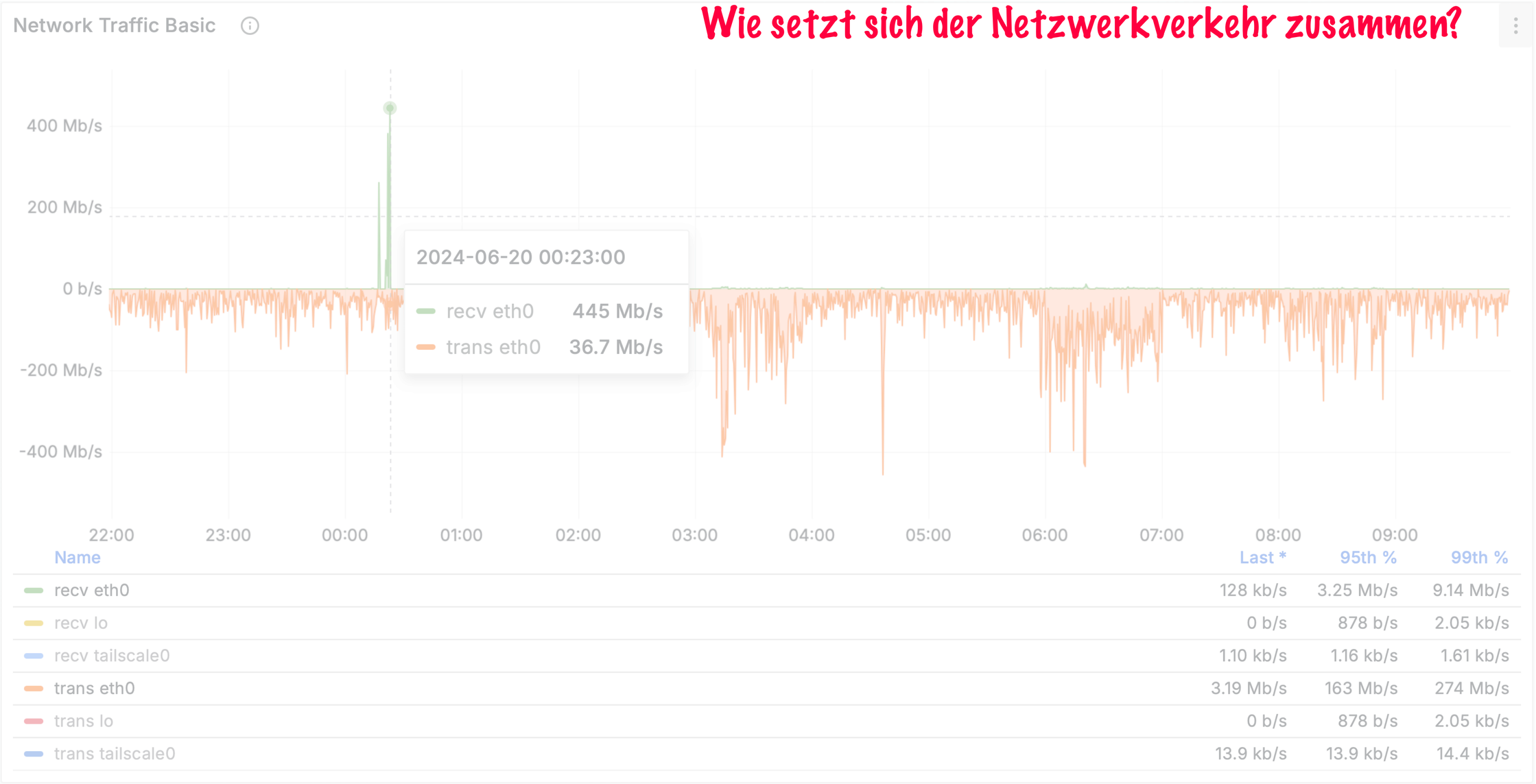
🍎 🥕

Network Flows in a Nutshell

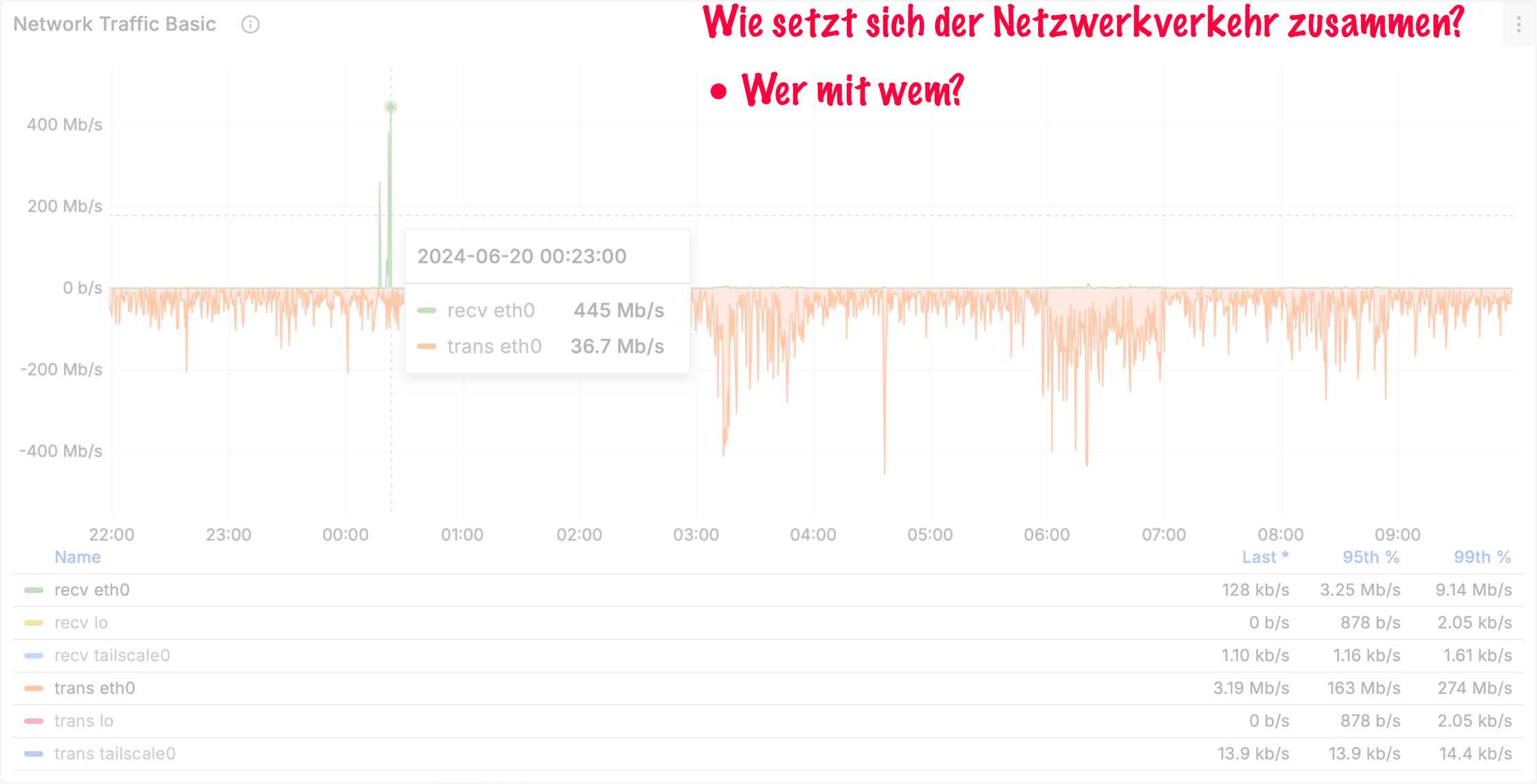


Network Flows in a Nutshell

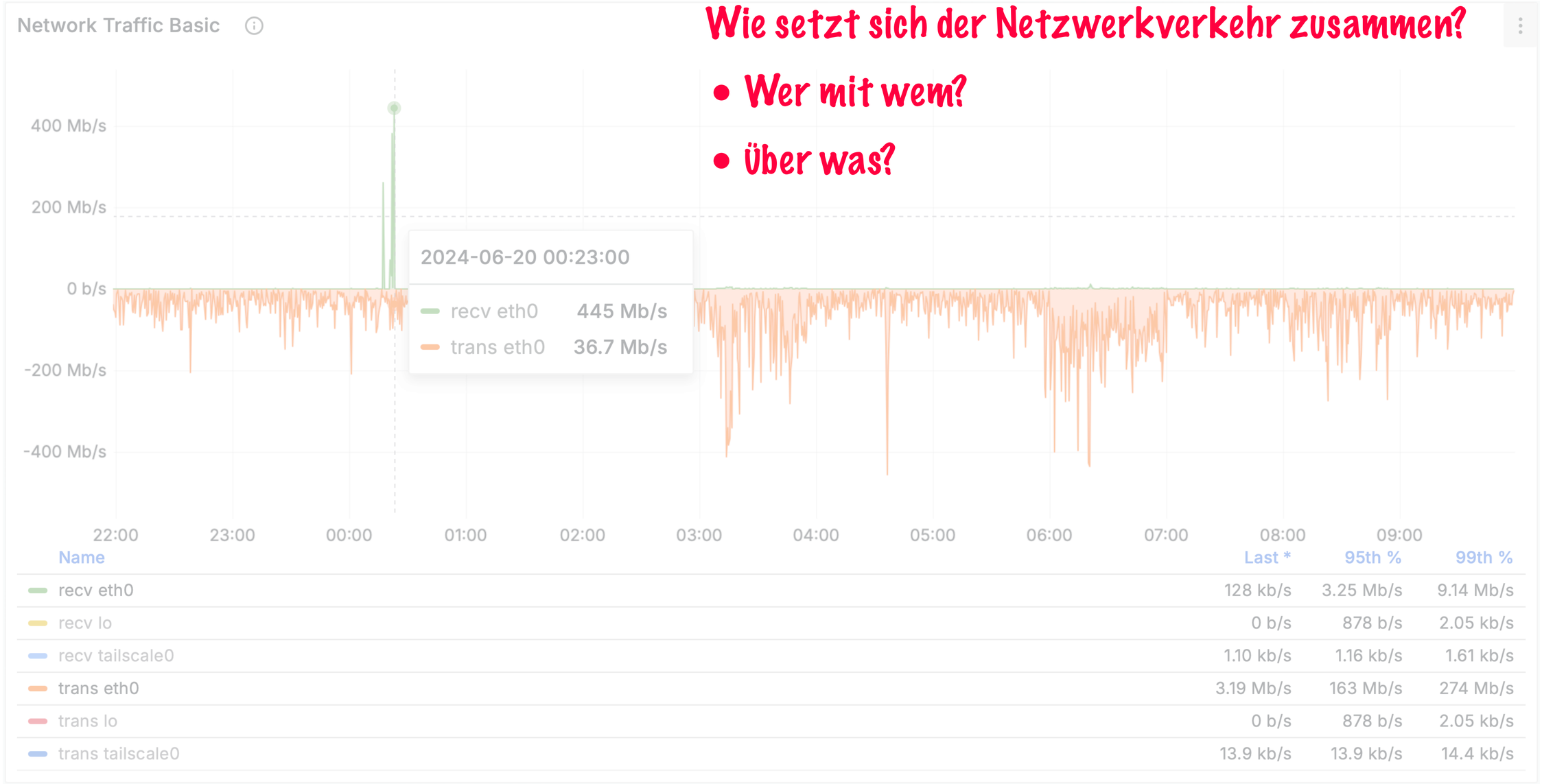
Wie setzt sich der Netzwerkverkehr zusammen?



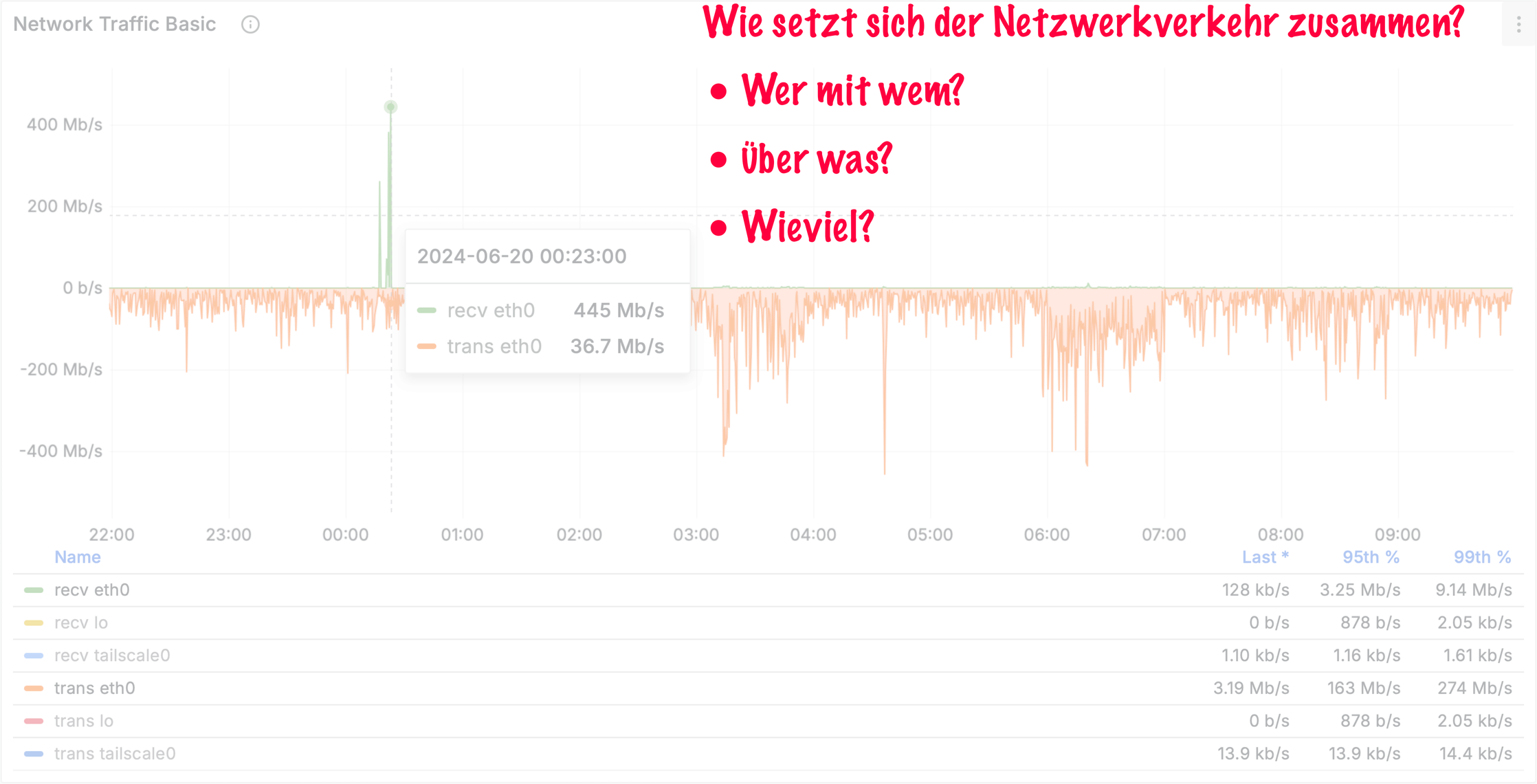
Network Flows in a Nutshell



Network Flows in a Nutshell



Network Flows in a Nutshell



Network Flows in a Nutshell

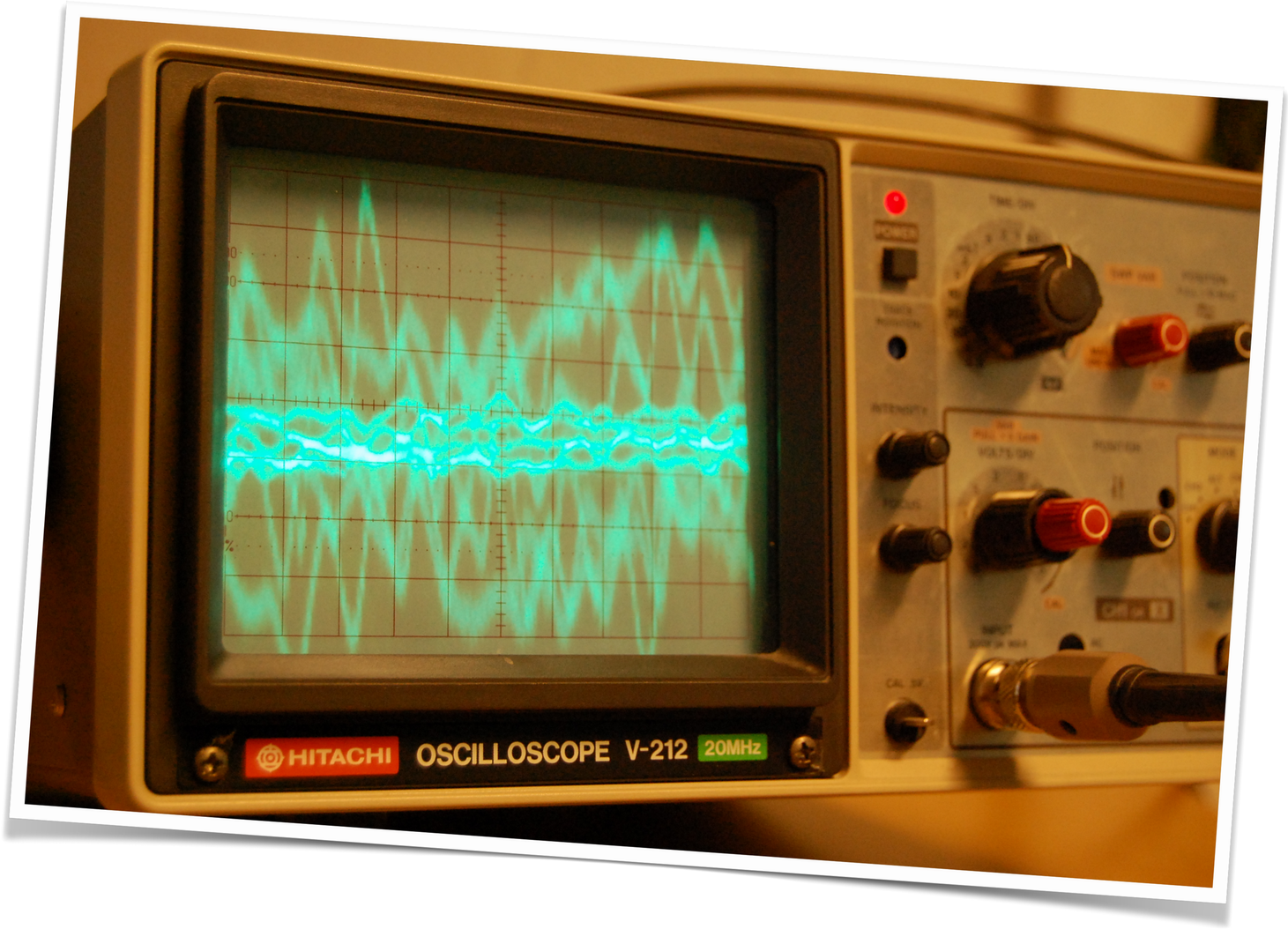
Wie setzt sich der Netzwerkverkehr zusammen?

- Wer mit wem?
- Über was?
- Wieviel?

	Last *	95th %	99th %
	128 kb/s	3.25 Mb/s	9.14 Mb/s
	0 b/s	878 b/s	2.05 kb/s
	1.10 kb/s	1.16 kb/s	1.61 kb/s
	3.19 Mb/s	163 Mb/s	274 Mb/s
trans lo	0 b/s	878 b/s	2.05 kb/s
trans tailscale0	13.9 kb/s	13.9 kb/s	14.4 kb/s

Fehleranalyse

- Wer verursacht Überlastung
- Wer ist betroffen



Kapazitätsplanung

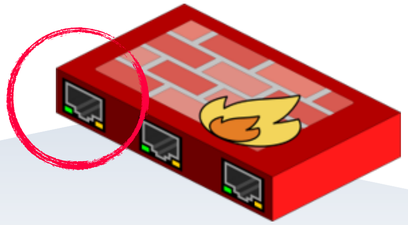
Von wo nach wo brauch ich mehr

Kapazität?

Sicherheit

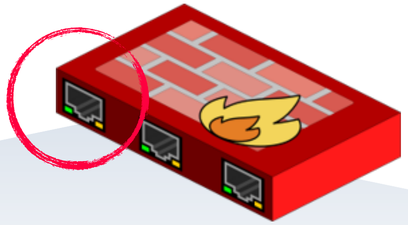
Gibt es Netzwerkverkehr der da nicht sein dürfte?

Was ist ein flow?



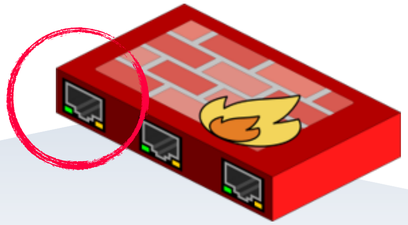
Source IP	Destination IP	Source Port	Destination Port	Interface	Protocol	Bytes

Was ist ein flow?



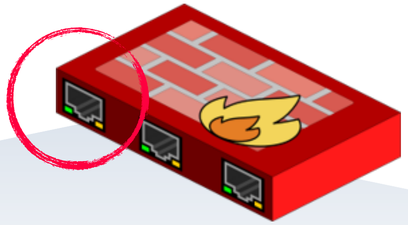
Source IP	Destination IP	Source Port	Destination Port	Interface	Protocol	Bytes
192.168.1.23	104.125.70.17	38274	443	1	6	**400**

Was ist ein flow?



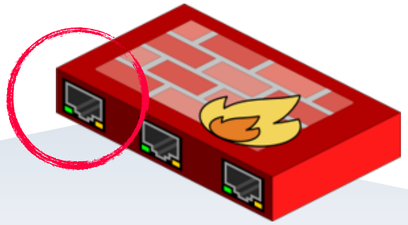
Source IP	Destination IP	Source Port	Destination Port	Interface	Protocol	Bytes
192.168.1.23	104.125.70.17	38274	443	1	6	**520**
192.168.1.42	52.202.62.232	23455	443	1	6	**350**

Was ist ein flow?



Source IP	Destination IP	Source Port	Destination Port	Interface	Protocol	Bytes
192.168.1.23	104.125.70.17	38274	443	1	6	**610**
192.168.1.42	52.202.62.232	23455	443	1	6	**420**
192.168.1.40	172.217.42.211	11244	27960	1	17	**512**

Was ist ein flow?

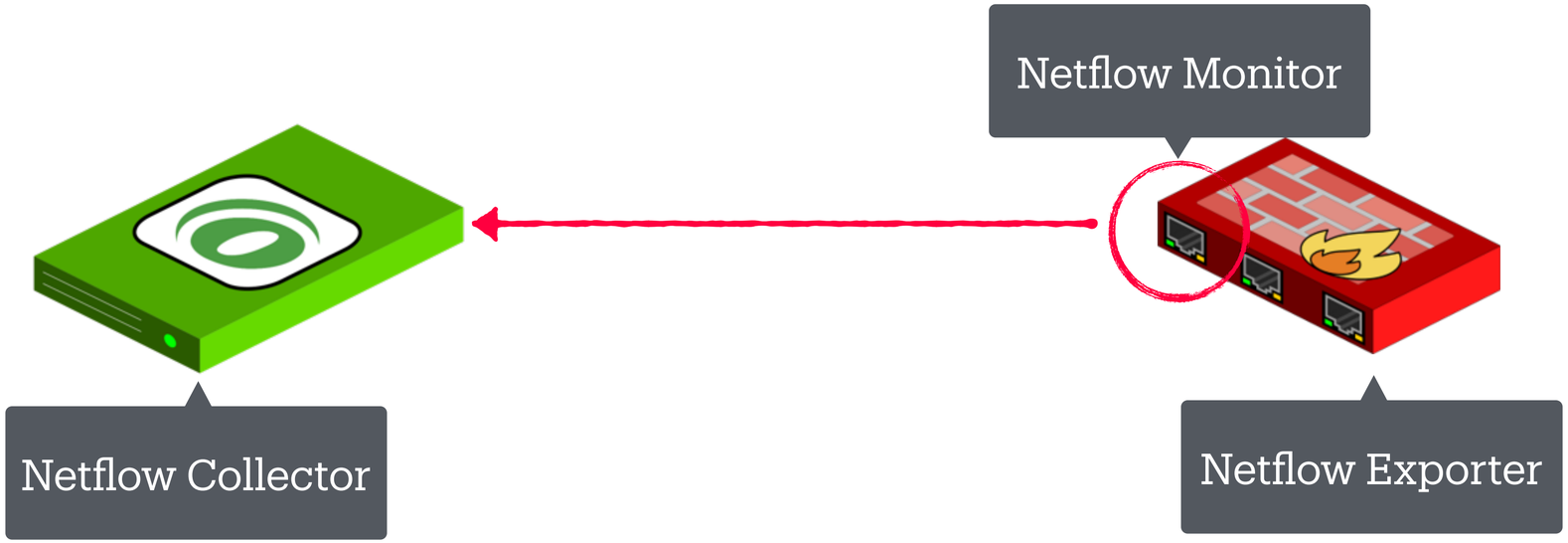


Source IP	Destination IP	Source Port	Destination Port	Interface	Protocol	Bytes
192.168.1.23	104.125.70.17	38274	443	1	6	**870**
192.168.1.42	52.202.62.232	23455	443	1	6	**620**
192.168.1.40	172.217.42.211	11244	27960	1	17	**1536**
192.168.1.102	52.210.67.110	21234	993	1	6	**2354**

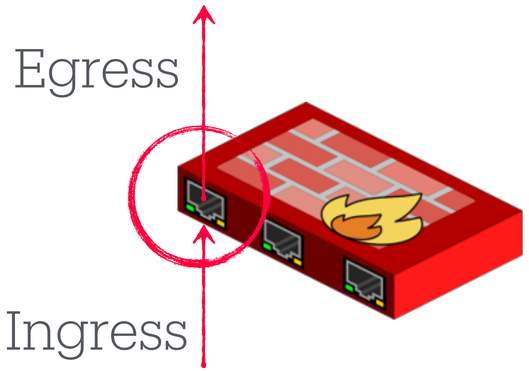
Was ist ein flow?

Source IP	Destination IP	Source Port	Destination Port	Interface	Protocol	Bytes
192.168.1.23	104.125.70.17	38274	443	1	6	**1240**
192.168.1.42	52.202.62.232	23455	443	1	6	**920**
192.168.1.40	172.217.42.211	11244	27960	1	17	**2540**
192.168.1.102	52.210.67.110	21234	993	1	6	**3750**

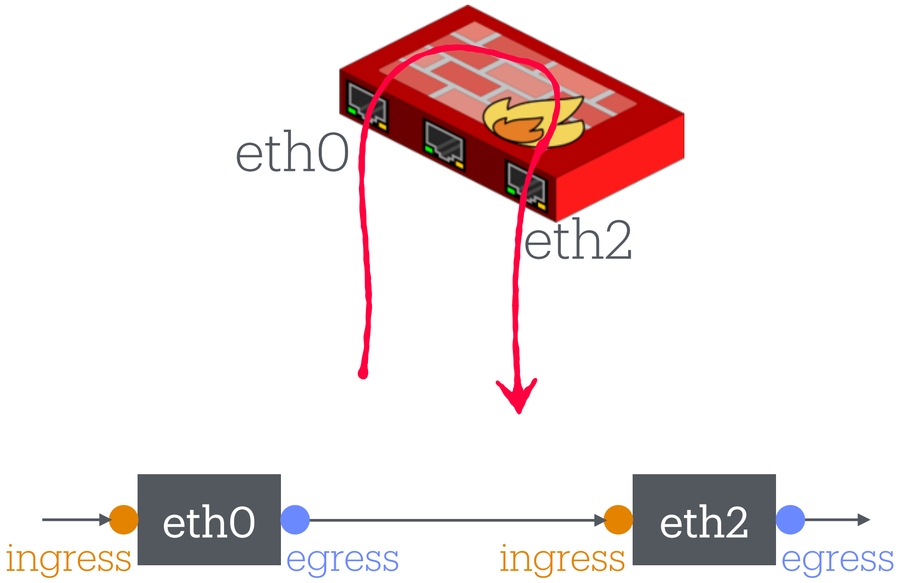
Was ist ein flow?



Was ist ein flow?



Was ist ein flow?



Netflow Verarbeiten

Adapter

Parser

Listener

- IPv4/IPv6
- UDP
- TCP

Netflow Verarbeiten

Adapter

Parser

- Netflow v5
- Netflow v9
- IPFIX
- sFlow

Listener

2055/udp
9999/udp
4739/udp
6343/udp

Netflow Verarbeiten

Adapter

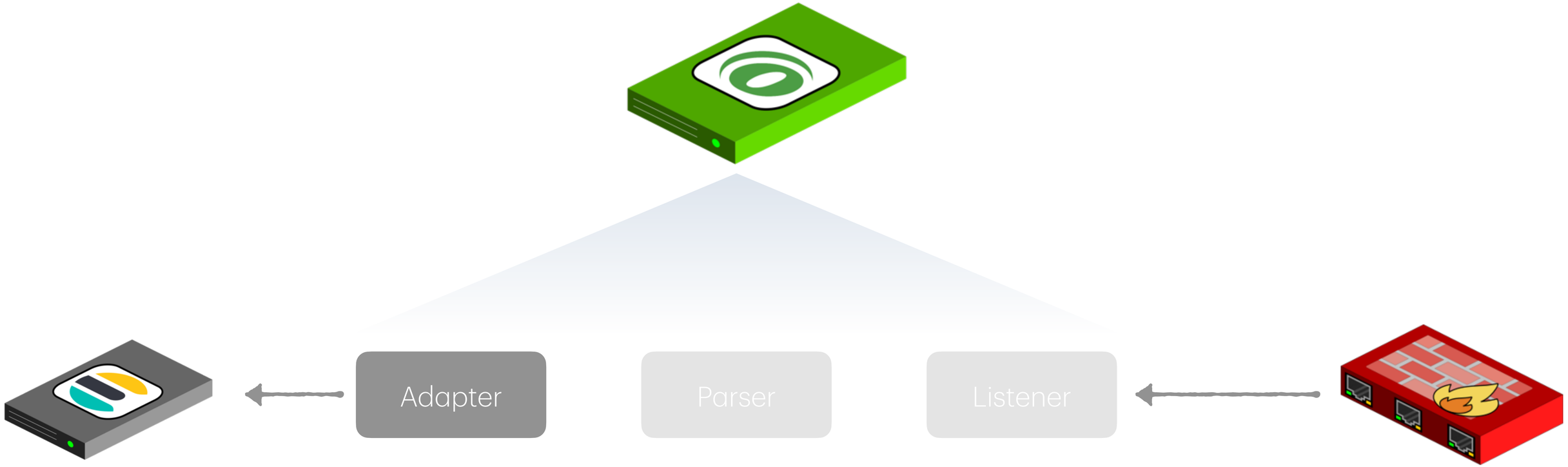
Parser

Listener

- Netflow v5
- Netflow v9
- IPFIX
- sFlow

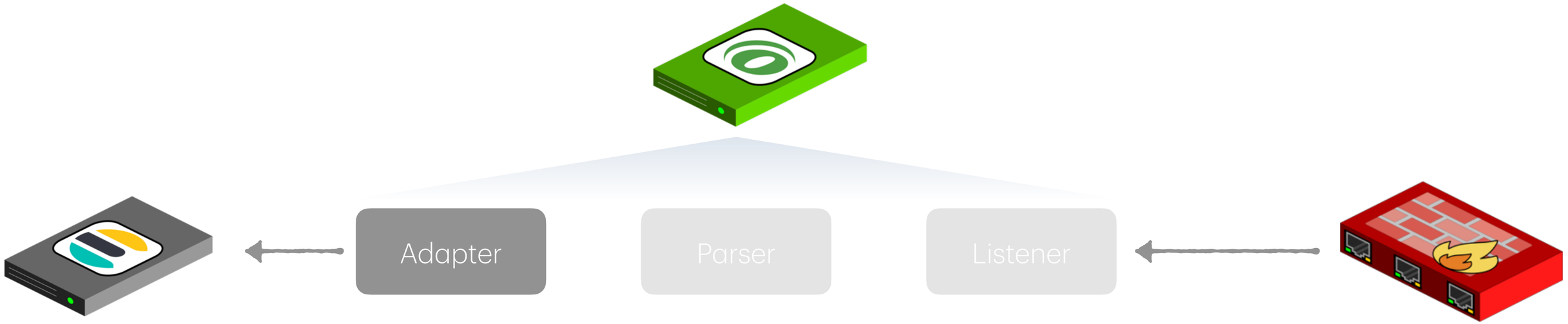
9999/UDP

Netflow Verarbeiten



- Flow Dokumente
- Anreicherung

Flows anreichern

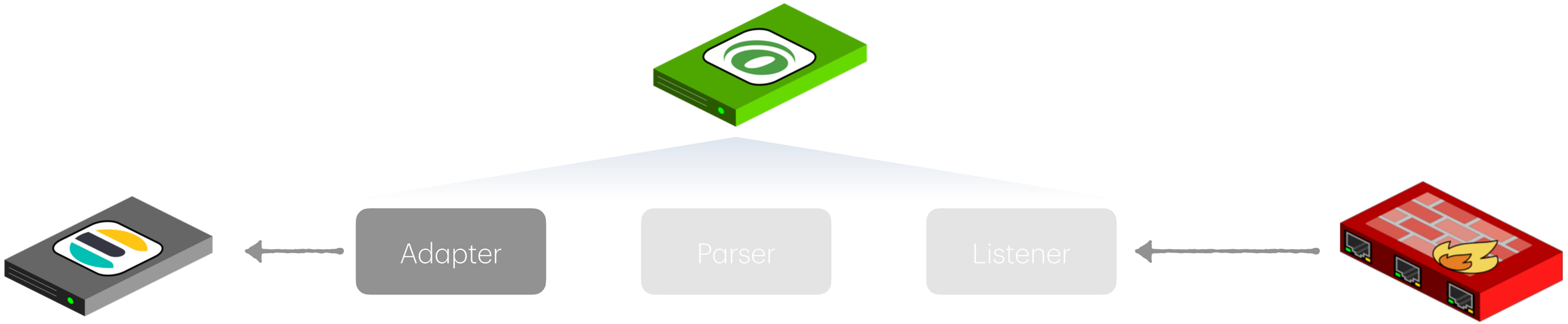


Source IP	Destination IP	Source Port	Destination Port	Interface	Protocol	Bytes
192.168.1.23	104.125.70.17	38274	443	1	6	**400**

your.box.at.your.corp

cdn.playstation.com

Flows anreichern



Source IP	Destination IP	Source Port	Destination Port	Interface	Protocol	Bytes
192.168.1.23	104.125.70.17	38274	443	1	6	**400**

your.box.at.your.corp

cdn.playstation.com

OpenNMS Inventar

- https
- Categories
- eth0
- Location
- tcp
- Inventar ID's

Node Interfaces

IP Interfaces | SNMP Interfaces

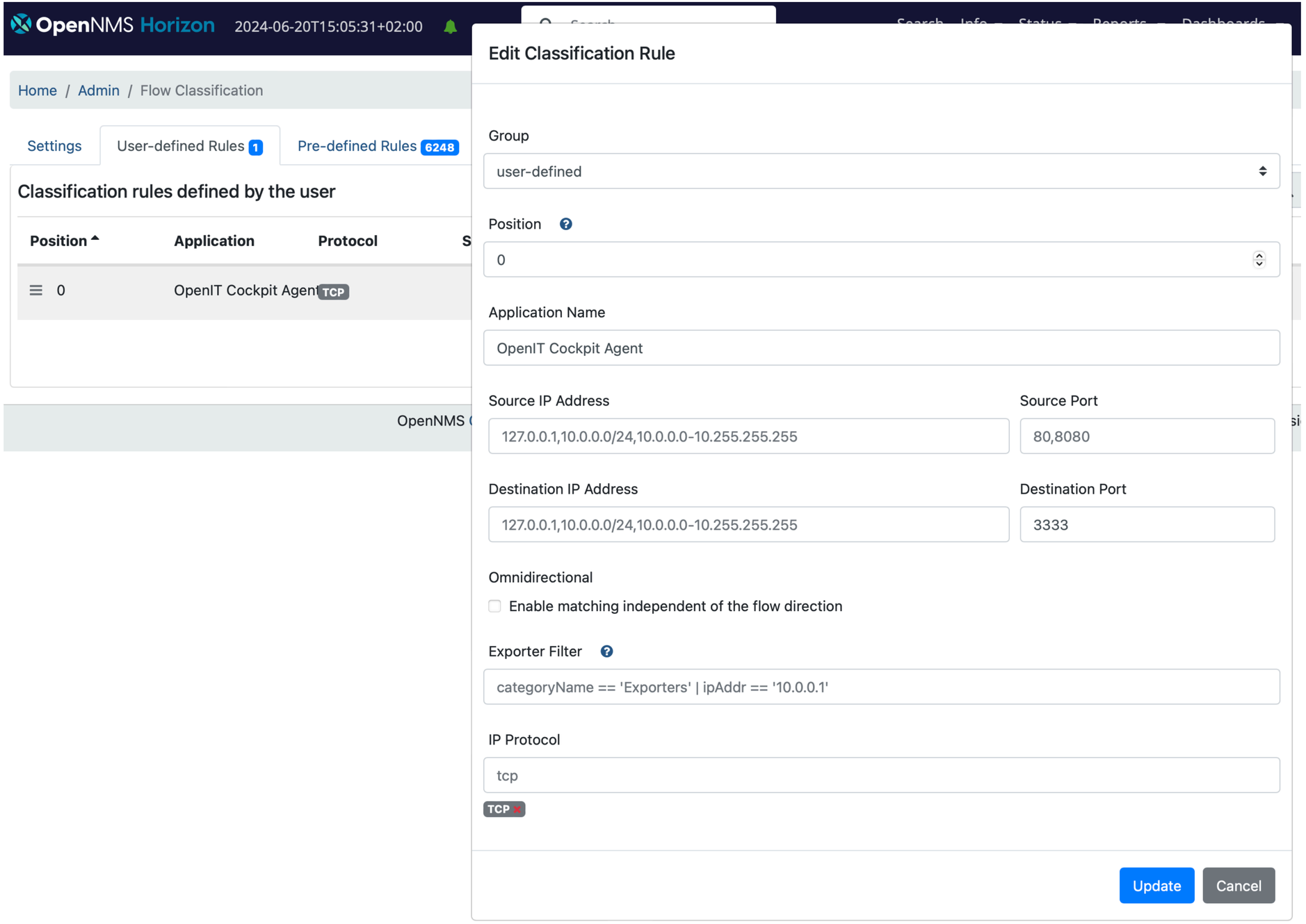
Search/Filter SNMP Interfaces

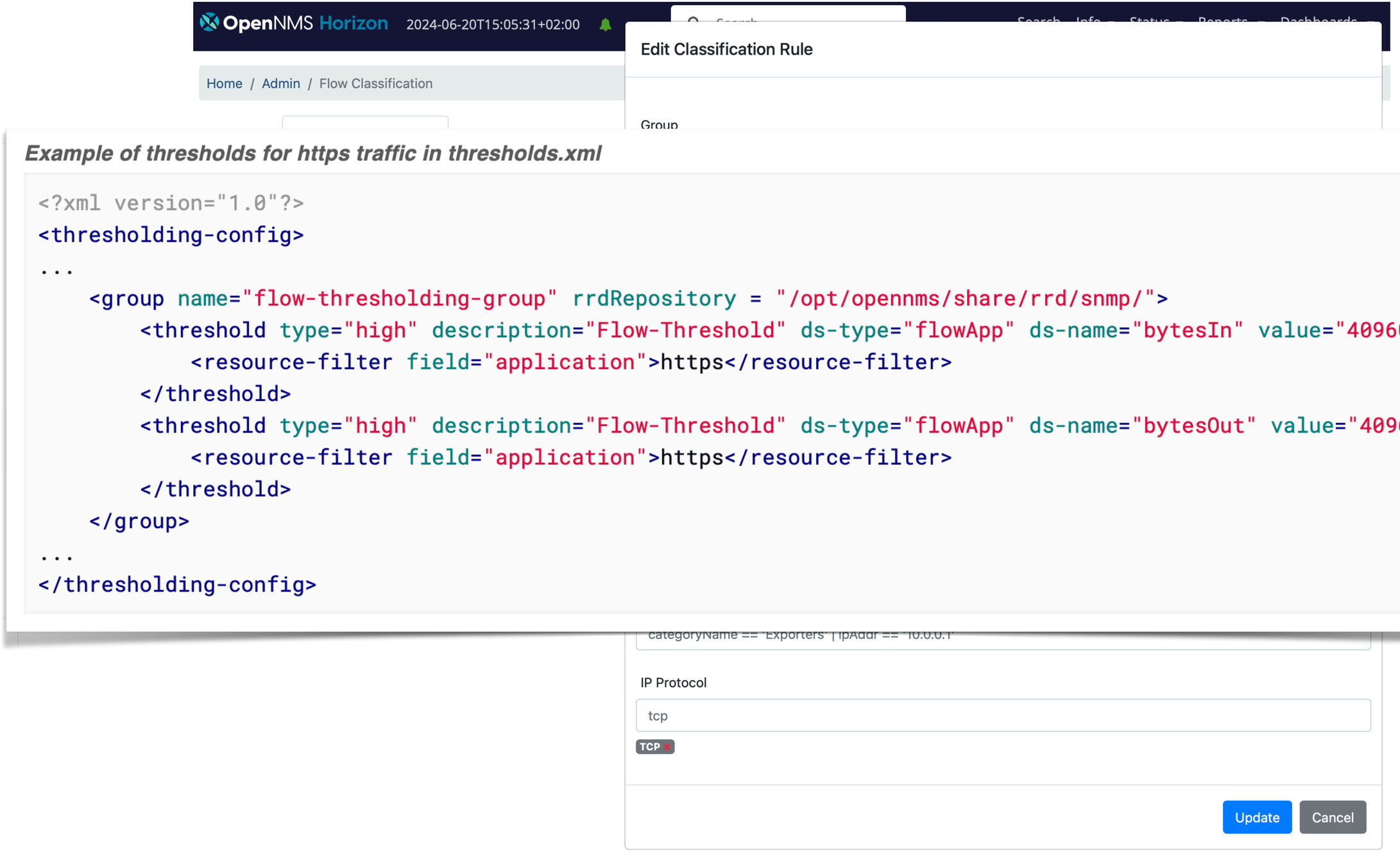
SNMP ifIndex	SNMP ifDescr	SNMP ifName	SNMP ifAlias	SNMP ifSpeed
1	lo	lo	lo	10000000
2	eth3	eth3	sfp-fiber	10000000
3	eth0	eth0	isp	1000000000
4	eth1	eth1	home	1000000000
5	eth2	eth2	labmonkeys	1000000000
6	npi0	npi0	npi0	N/A
7	npi1	npi1	npi1	N/A
8	npi2	npi2	npi2	N/A
9	npi3	npi3	npi3	N/A
10	loop0	loop0	loop0	N/A

First | Previous | 1 | 2 | Next | Last

S	Bytes
192	400

your.box


OpenNMS Horizon
2024-06-20T15:05:31+02:00
Search
Info
Status
Reports
Dashboards
Home / Admin / Flow Classification
Settings
User-defined Rules 1
Pre-defined Rules 6248
Classification rules defined by the user
Position
Application
Protocol
0
OpenIT Cockpit Agent
TCP
OpenNMS
Edit Classification Rule
Group
user-defined
Position
0
Application Name
OpenIT Cockpit Agent
Source IP Address
127.0.0.1,10.0.0.0/24,10.0.0.0-10.255.255.255
Source Port
80,8080
Destination IP Address
127.0.0.1,10.0.0.0/24,10.0.0.0-10.255.255.255
Destination Port
3333
Omnidirectional
Enable matching independent of the flow direction
Exporter Filter
categoryName == 'Exporters' | ipAddr == '10.0.0.1'
IP Protocol
tcp
TCP
Update
Cancel



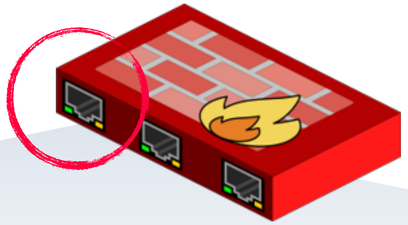
Example of thresholds for https traffic in thresholds.xml

XML

```
<?xml version="1.0"?>
<thresholding-config>
...
    <group name="flow-thresholding-group" rrdRepository = "/opt/opennms/share/rrd/snmp/">
        <threshold type="high" description="Flow-Threshold" ds-type="flowApp" ds-name="bytesIn" value="4096000" rearm="2
            <resource-filter field="application">https</resource-filter>
        </threshold>
        <threshold type="high" description="Flow-Threshold" ds-type="flowApp" ds-name="bytesOut" value="4096000" rearm='
            <resource-filter field="application">https</resource-filter>
        </threshold>
    </group>
...
</thresholding-config>
```

Netflow v5	Netflow v9	IPFIX	sFlow
Cisco	Cisco (RFC 3954)	Open (RFC 7012)	Open (RFC 3176)
Flow based or sampled	Flow based or sampled	Flow based or sampled	Sampled
Ingress Only	Ingress/Egress	Ingress/Egress	Ingress/Egress
IPv4	IPv4/IPv6/VLAN/MPLS	IPv4/IPv6/VLAN/MPLS	IPv4/IPv6/VLAN/MPLS
Static	Extensible	Extensible	Extensible

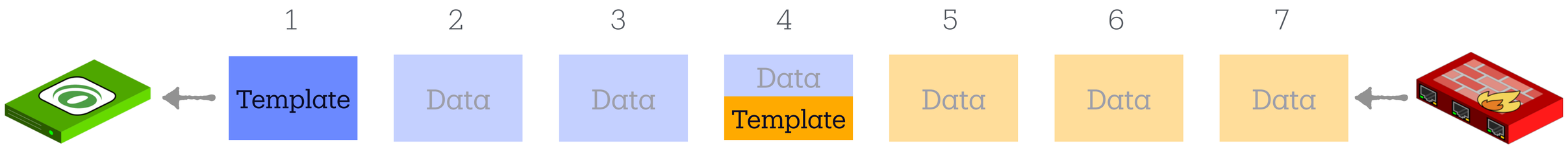
Flow extension



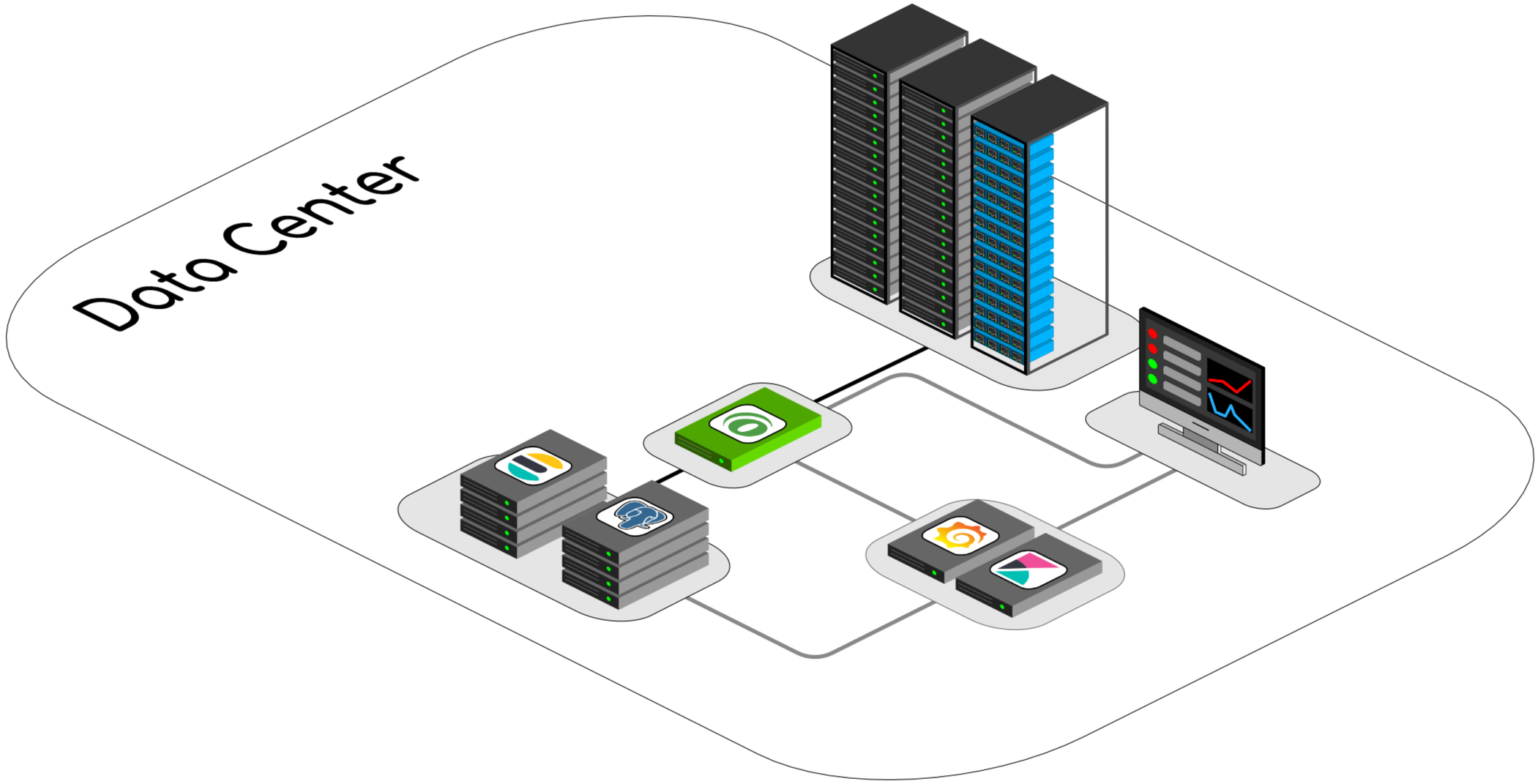
Source IP	Destination IP	Source Port	Destination Port	Interface	Protocol	Bytes

Routing Source AS	Source autonomous system number.
Routing Destination AS	Destination autonomous system number.
Routing Next-hop Address	IP address of the next hop.
IP Source Mask	Mask for the IP source address.
IP Destination Mask	Mask for the IP destination address.
Transport TCP Flags	Value in the TCP flag field.

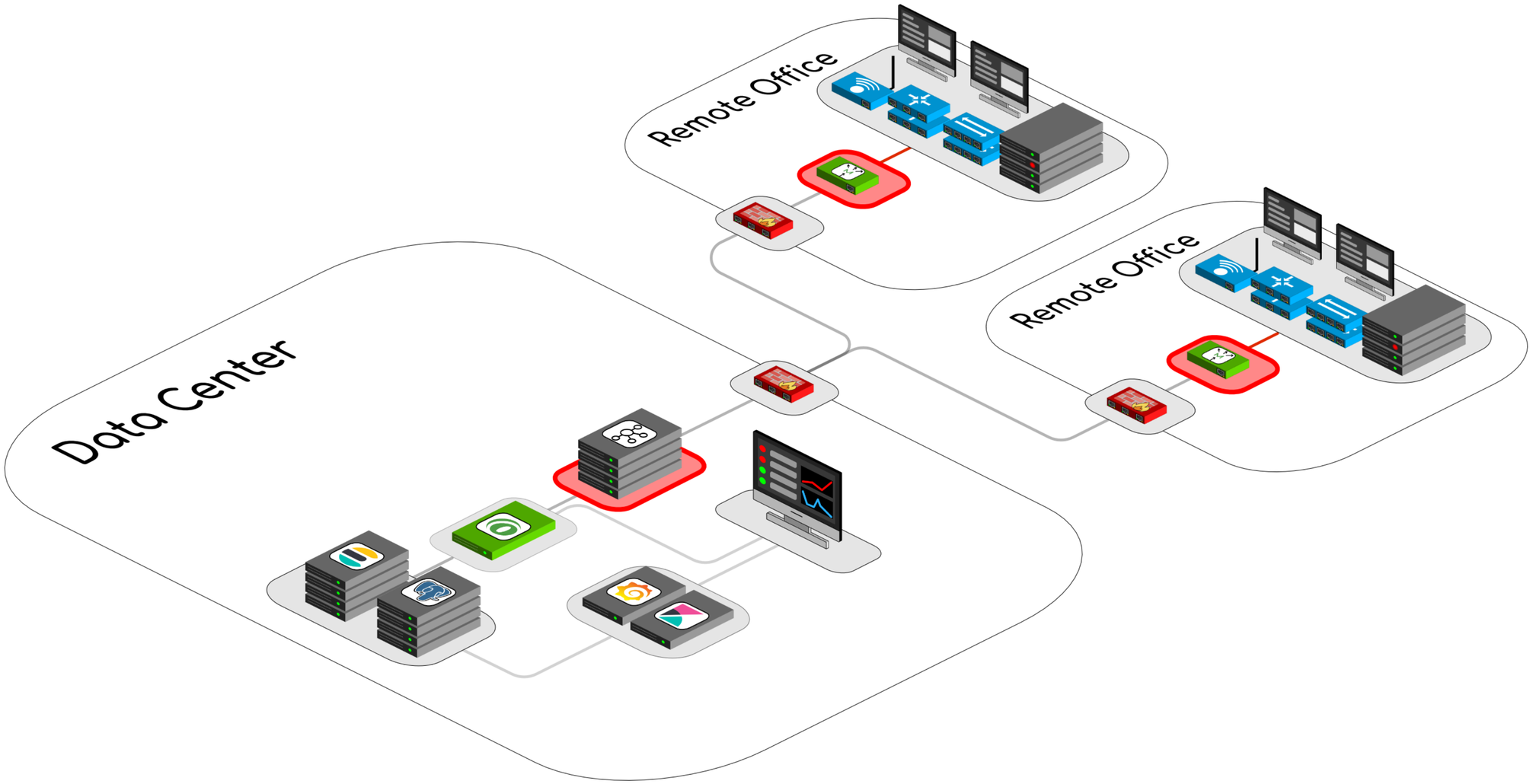
Flow Extension



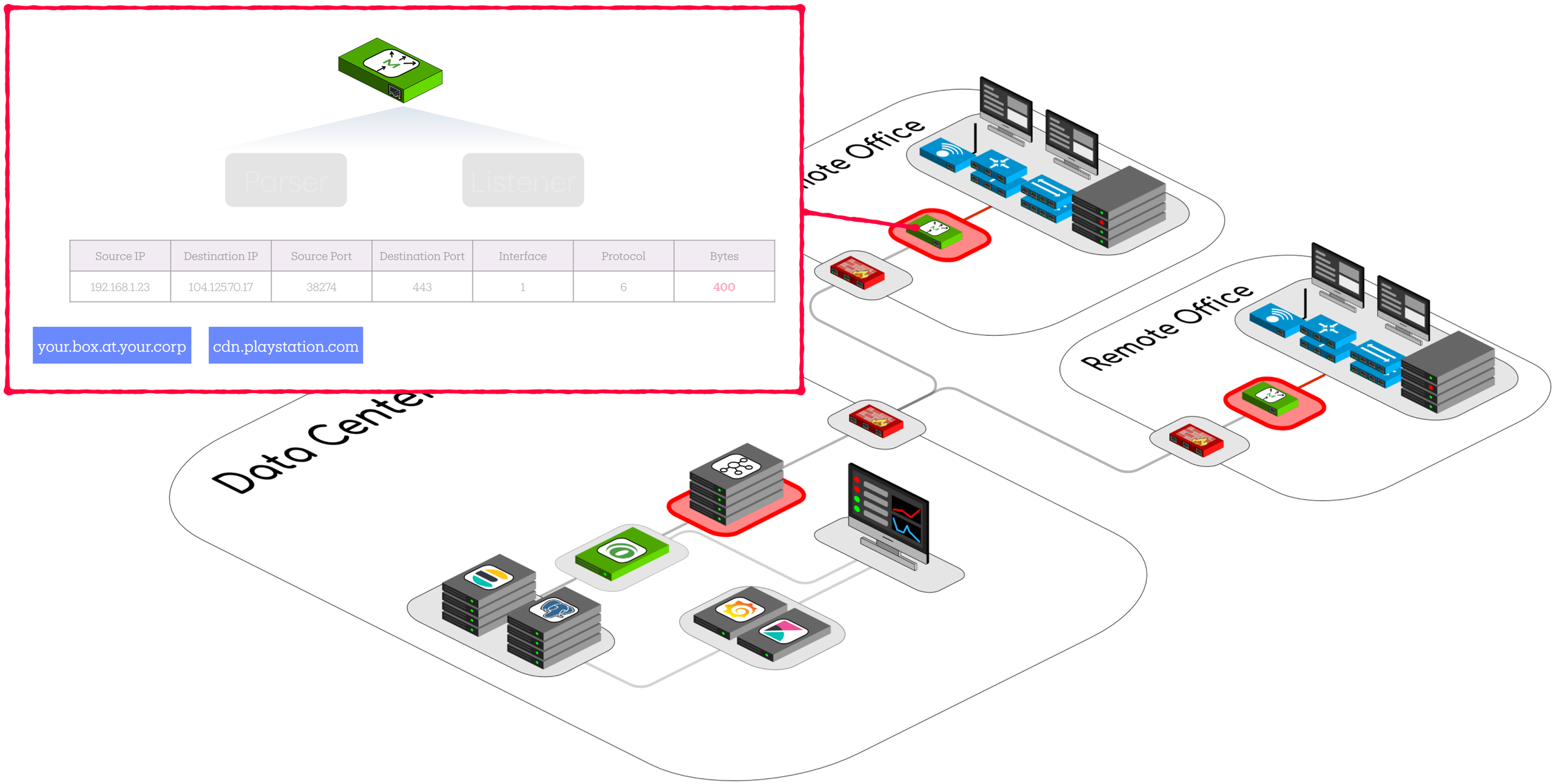
Local Network



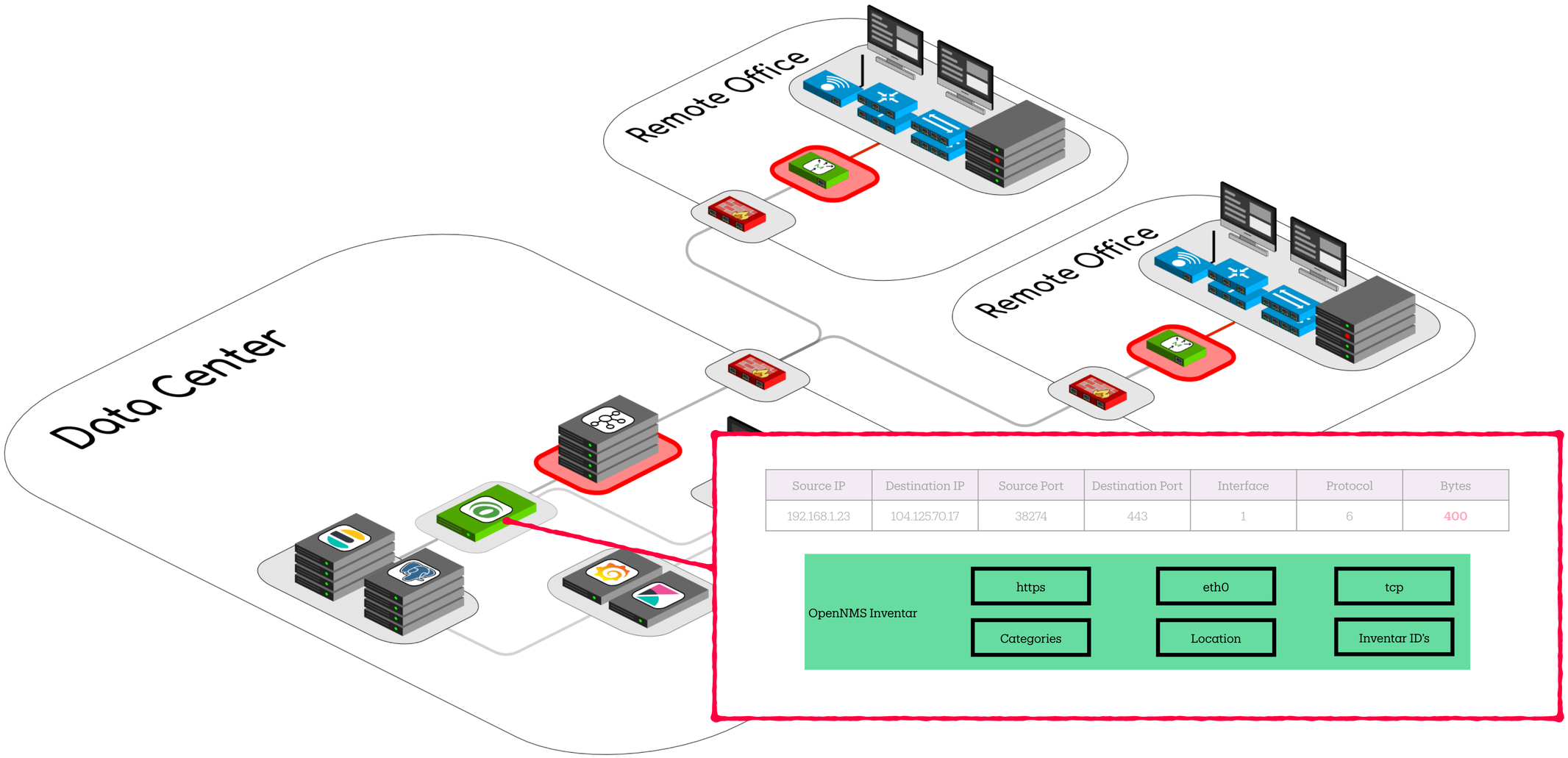
Distributed Deployment



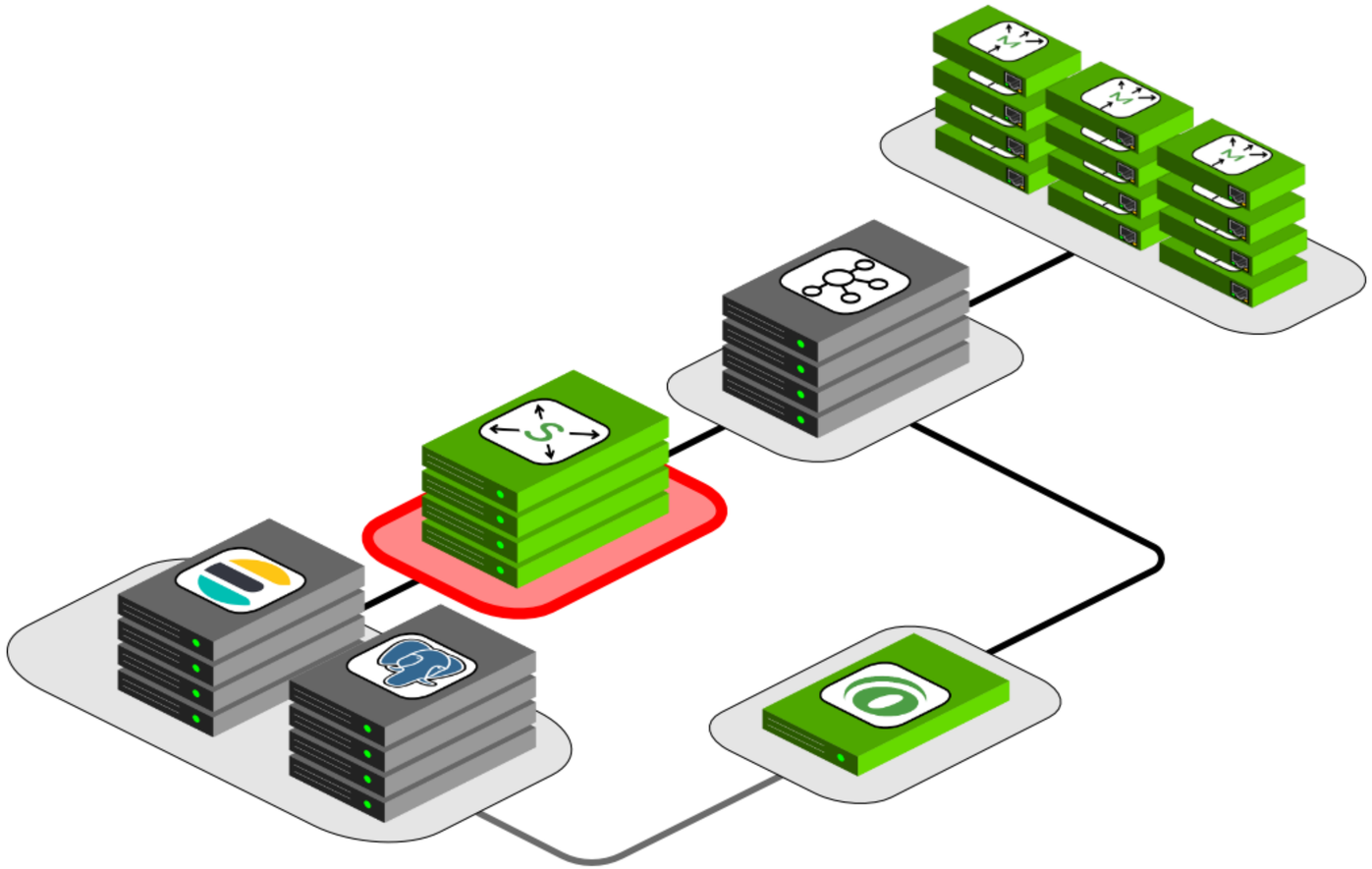
Distributed Deployment



Distributed Deployment



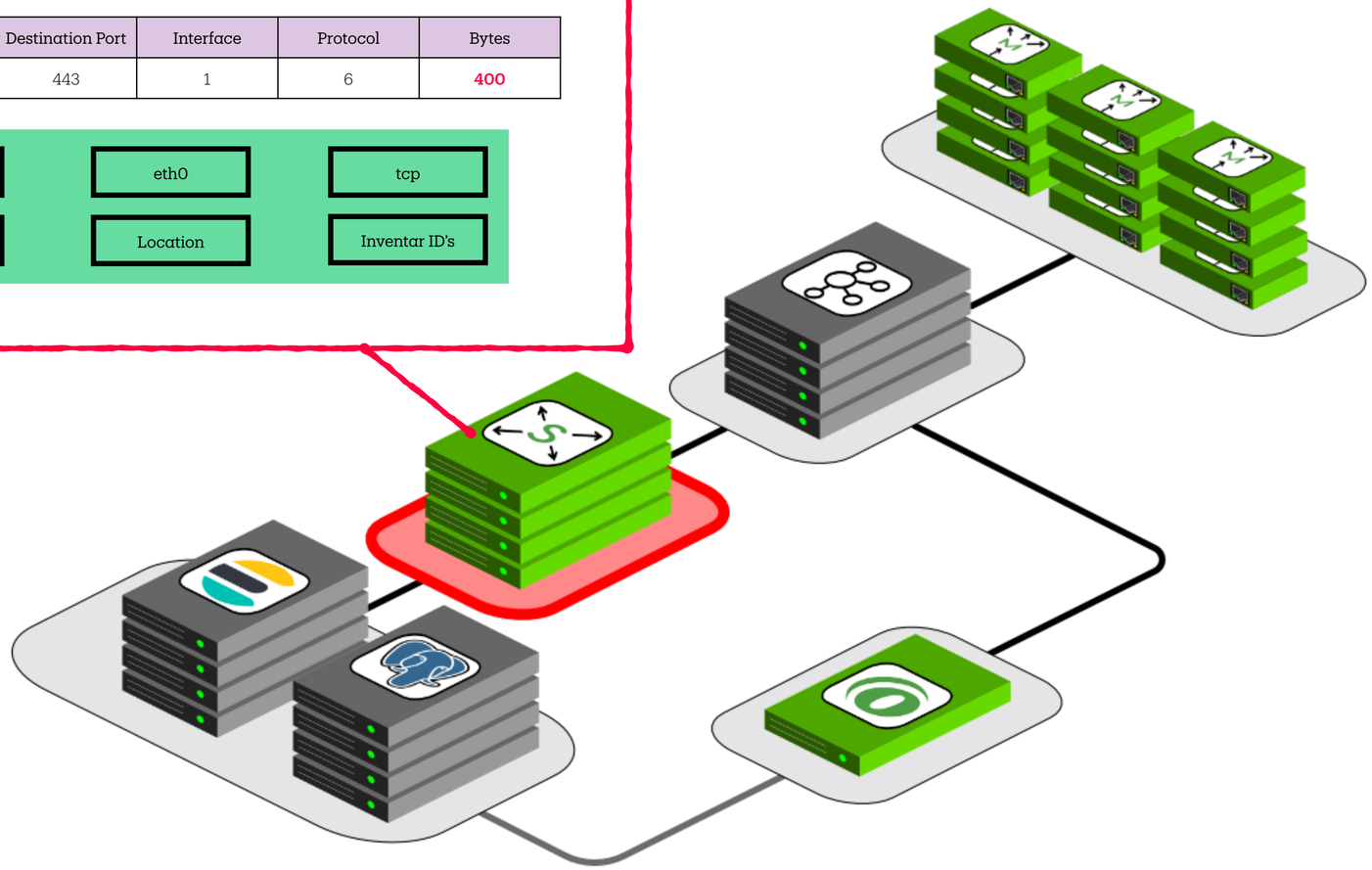
Large Volume Deployment



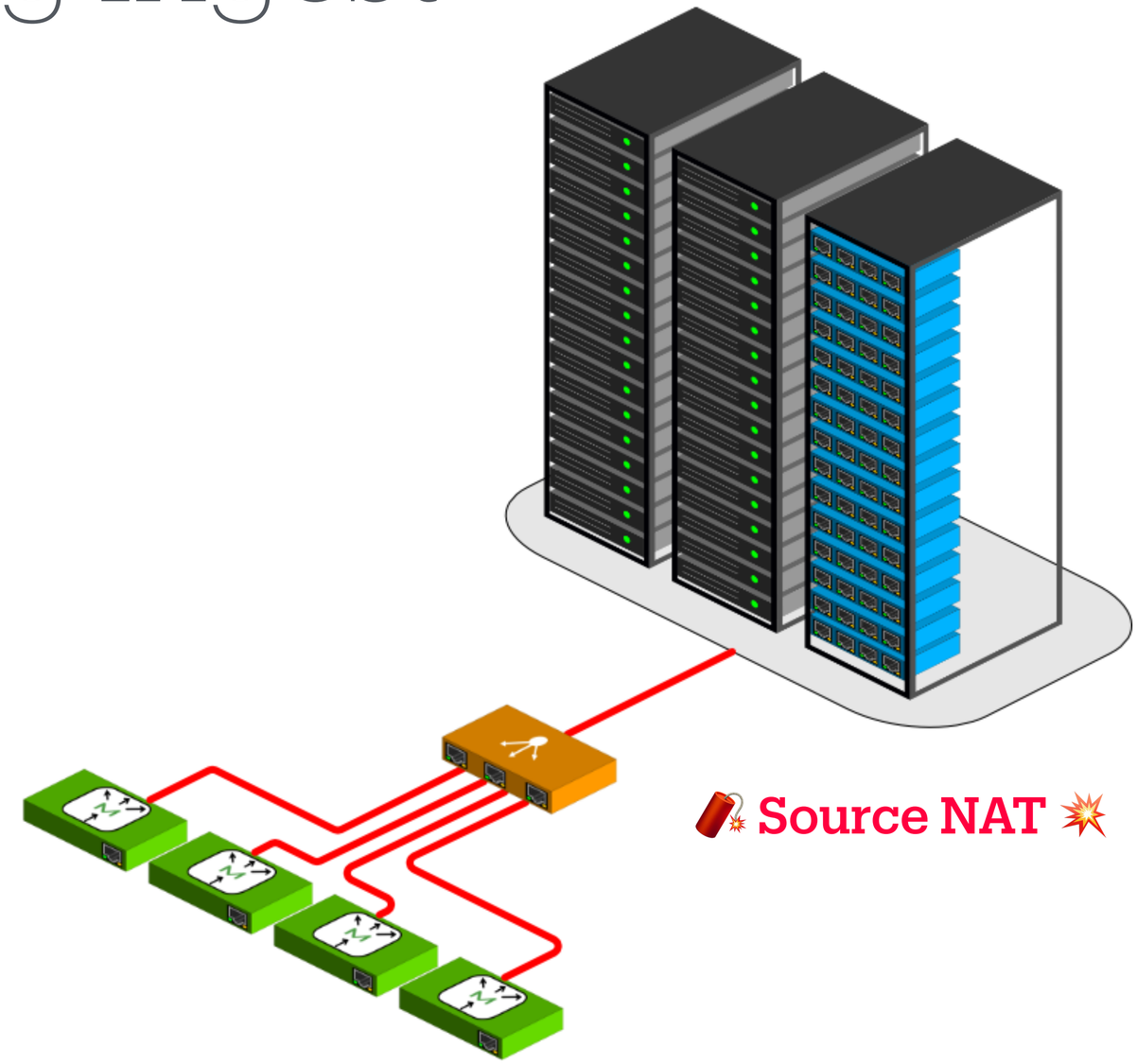
Large Volume Deployment

Source IP	Destination IP	Source Port	Destination Port	Interface	Protocol	Bytes
192.168.1.23	104.125.70.17	38274	443	1	6	400

OpenNMS Inventar	https	eth0	tcp
	Categories	Location	Inventar ID's

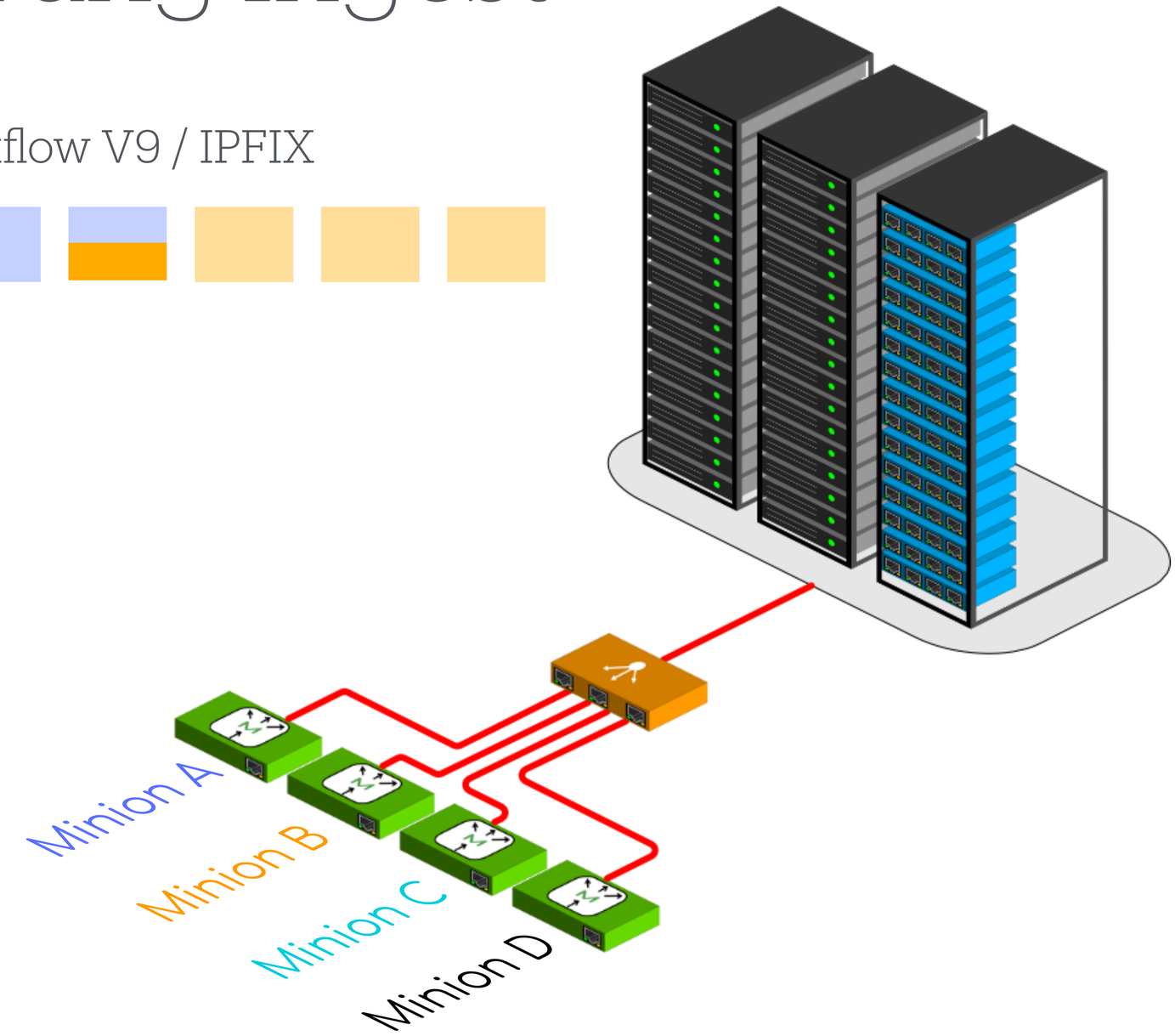


Skalierung Ingest



Skalierung Ingest

Templates Netflow V9 / IPFIX



Skalierung Ingest

Templates Netflow V9 / IPFIX

Search or jump to... ⌘+k

Home › Administration › Plugins and data › Plugins

Plugins

Extend the Grafana experience with panel plugins and apps. To find more data sources go to Connections.

Search: openn × Clear

Type: All

State: All | Installed

Sort: By name (A-Z)

View

Grafana Enterprise Traces
By Grafana Labs
Signed | Enterprise

Highlight.io
By highlight.io
Signed

LLM
By Grafana Labs
Signed

openGemini
By opengemini
Signed

openHistorian
By Grid Protection Alliance
Signed | Angular

OpenNMS Plugin for Grafana
By The OpenNMS Group Inc.
Signed | Installed

OpenSearch
By Grafana Labs
Signed

OpenTSDB
By Grafana Labs
Core | Installed

Pixie Grafana Datasource Plugin
By pixie
Signed

ServiceNow Cloud Observability
By servicenow
Signed

Search or jump to... ⌘+k

Home › Connections › Data sources

Elasticsearch
Elasticsearch | http://elastic-01.labmonkeys.tech:9200
Build a dashboard | Explore

fetzerch-sunandmoon-datasource
Sun and Moon
Build a dashboard | Explore

Grafana Pyroscope
Grafana Pyroscope | http://dinky.labmonkeys.tech:4040
Build a dashboard | Explore

mimir.labmonkeys.tech
Prometheus | http://mimir.labmonkeys.tech:9009/prometheus
Build a dashboard | Explore

OpenNMS Entities
OpenNMS Entities | http://hzn-core-web-svc.app-onms-horizon.svc.cluster.local:8980/opennms
Build a dashboard | Explore

OpenNMS Flow
OpenNMS Flow | http://hzn-core-web-svc.app-onms-horizon.svc.cluster.local:8980/opennms
Build a dashboard | Explore

OpenNMS Performance
OpenNMS Performance | http://hzn-core-web-svc.app-onms-horizon.svc.cluster.local:8980/opennms
Build a dashboard | Explore

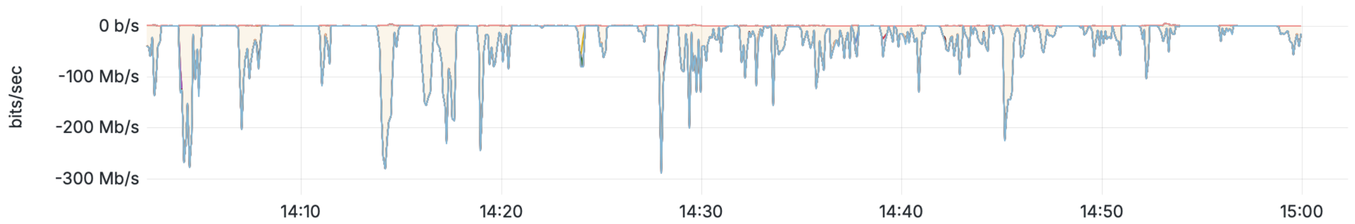
PostgreSQL
PostgreSQL | postgres.labmonkeys.tech:5432
Build a dashboard | Explore

Prometheus
Prometheus | http://tsdb.labmonkeys.tech:9009/prometheus | default
Build a dashboard | Explore

Flow Datasource: OpenNMS Flow | Perf. Datasource: OpenNMS Performance | Node: mirror | Interface: eth0(2) | DSCP: All

Flow Interface Statistics

Throughput by Application



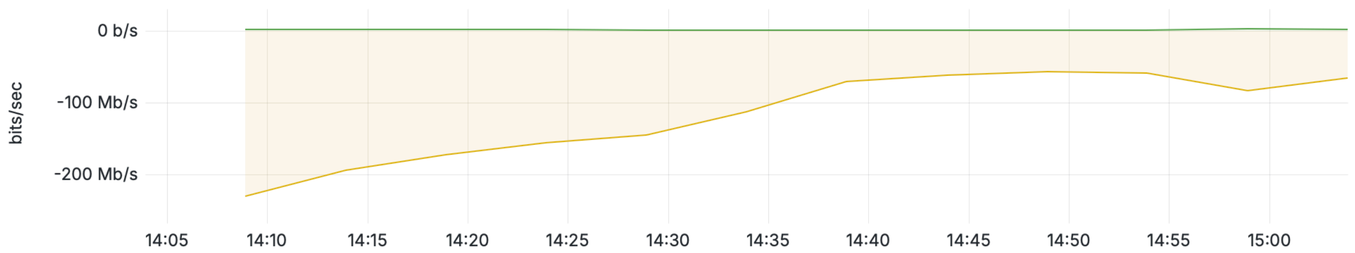
Name	Mean	Max	Min
https (In)	494 kb/s	4.87 Mb/s	0 b/s
https (Out)	-26.0 Mb/s	0 b/s	-290 Mb/s
[redacted]	-31.6 Mb/s	-5.58 Mb/s	-57.6 Mb/s

Data Usage by Application

Application	In	Out ↓
https	213.93 MB	11.28 GB
[redacted]	132.93 kB	44.16 MB
[redacted]	151.06 kB	39.21 MB
[redacted]	196.49 kB	32.40 MB
[redacted]	110.59 kB	30.54 MB
[redacted]	74.55 kB	13.52 MB

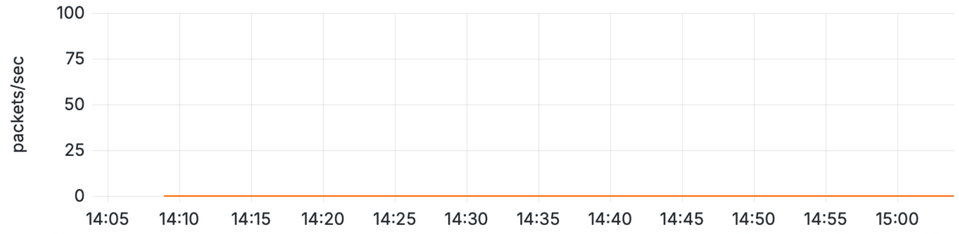
SNMP Interface Statistics

Interface Throughput



Name	Mean	Max	Min
Incoming	1.20 Mb/s	2.48 Mb/s	538 kb/s
Outgoing	118 Mb/s	230 Mb/s	57.7 Mb/s

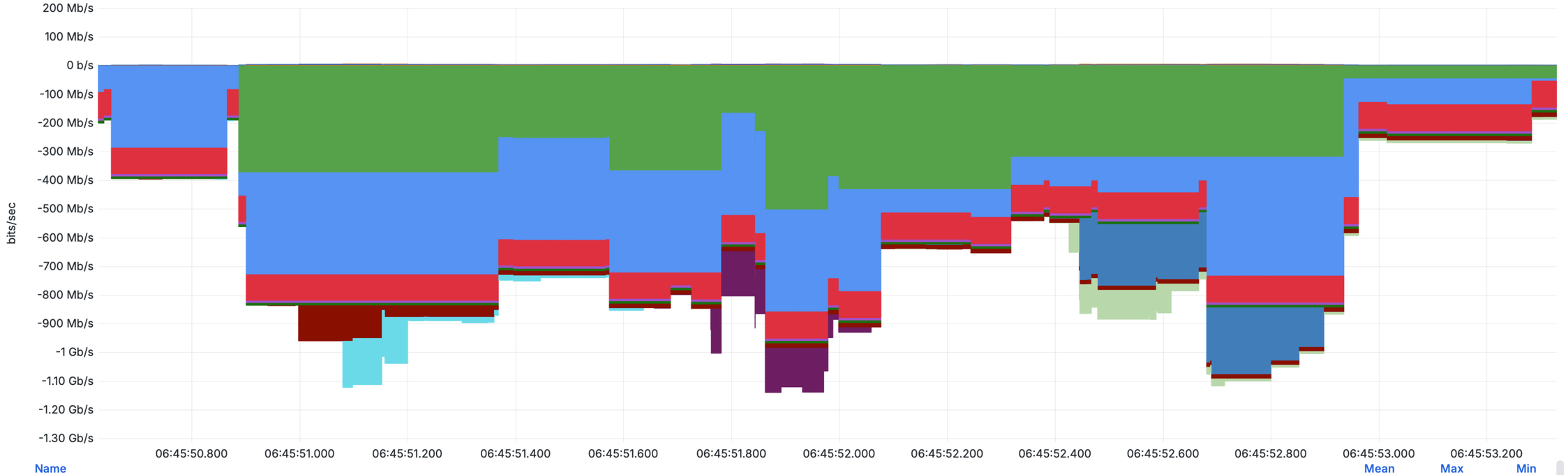
Errors and Discards



Name	Mean	Max	Min
ifInDiscards	0	0	0
ifOutErrors	0	0	0
ifInErrors	0	0	0

Flow Datasource: OpenNMS Flow | Perf. Datasource: OpenNMS Performance | Node: mirror | Interface: eth0(2) | DSCP: All

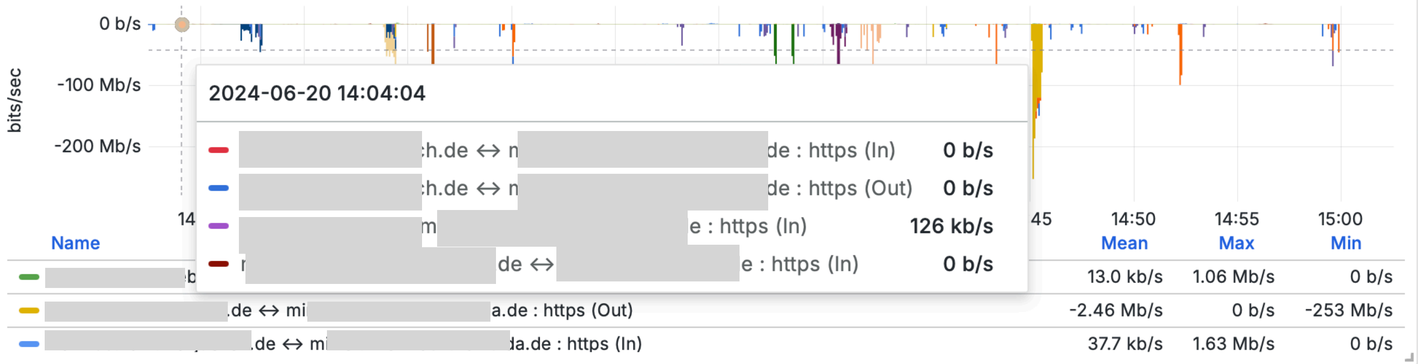
Throughput by Conversation (Top N)



Name	Mean	Max	Min
mirro[redacted]da.de ↔ 2a01[redacted]: https (Out)	-303 Mb/s	-44.8 Mb/s	-502 Mb/s
mirro[redacted]da.de ↔ 2a01[redacted]: https (In)	1.16 Mb/s	1.59 Mb/s	552 kb/s
mirro[redacted]da.de ↔ 2001:63[redacted]6 : https (Out)	-256 Mb/s	-8.22 Mb/s	-414 Mb/s
mirro[redacted]da.de ↔ 2001:63[redacted]6 : https (In)	978 kb/s	1.56 Mb/s	119 kb/s
if[redacted].de ↔ m[redacted]: https (Out)	-92.4 Mb/s	-44.9 Mb/s	-93.9 Mb/s
if[redacted].de ↔ m[redacted]: https (In)	1.67 Mb/s	1.70 Mb/s	807 kb/s
1[redacted]mi[redacted]: https (Out)	-8.29 Mb/s	-8.29 Mb/s	-8.29 Mb/s
1[redacted]mi[redacted]: https (In)	115 kb/s	115 kb/s	115 kb/s
m[redacted]-fulda.de ↔ 2[redacted]3 (Out)	-8.70 Mb/s	-8.70 Mb/s	-8.70 Mb/s
m[redacted]-fulda.de ↔ 2[redacted]3 (In)	151 kb/s	151 kb/s	151 kb/s
mirror.informatik.hs-fulda.de ↔ 2001:638:50e:125:1:7df2:0:1 : https (Out)	135 Mb/s	0 b/s	233 Mb/s

Conversation (Flows)

Throughput by Conversation (Top N)



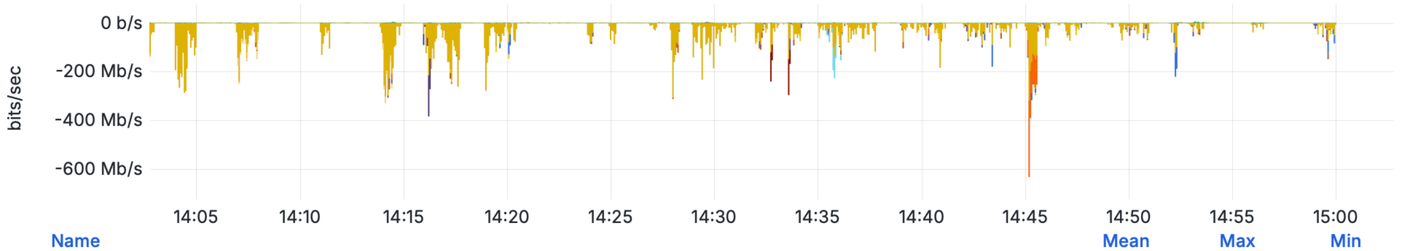
Name	Mean	Max	Min
b	13.0 kb/s	1.06 Mb/s	0 b/s
.de ↔ mi a.de : https (Out)	-2.46 Mb/s	0 b/s	-253 Mb/s
.de ↔ mi da.de : https (In)	37.7 kb/s	1.63 Mb/s	0 b/s

Data Usage by Conversation (Top N)

Source	Dest.	Application	In	Out
elich.de	m e	https	11.43 MB	310.74 MB
elich.de	m e	https	5.24 MB	258.84 MB
0	m e	https	4.47 MB	196.97 MB
da.de	52.230.152.243	https	1.12 MB	180.64 MB
da.de	52.230.152.45	https	979.22 kB	174.89 MB

Hosts (Flows)

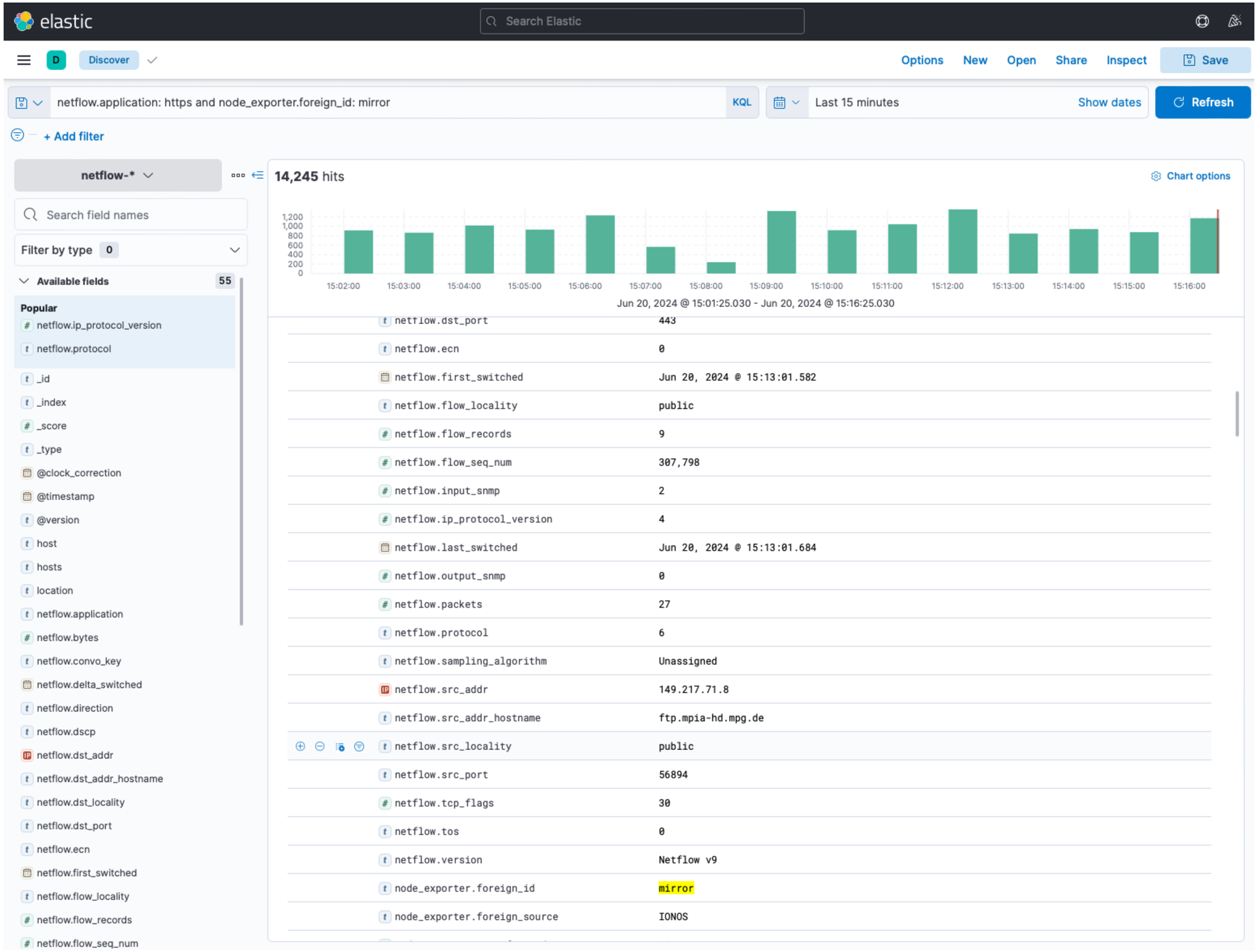
Throughput by Host (Top N)

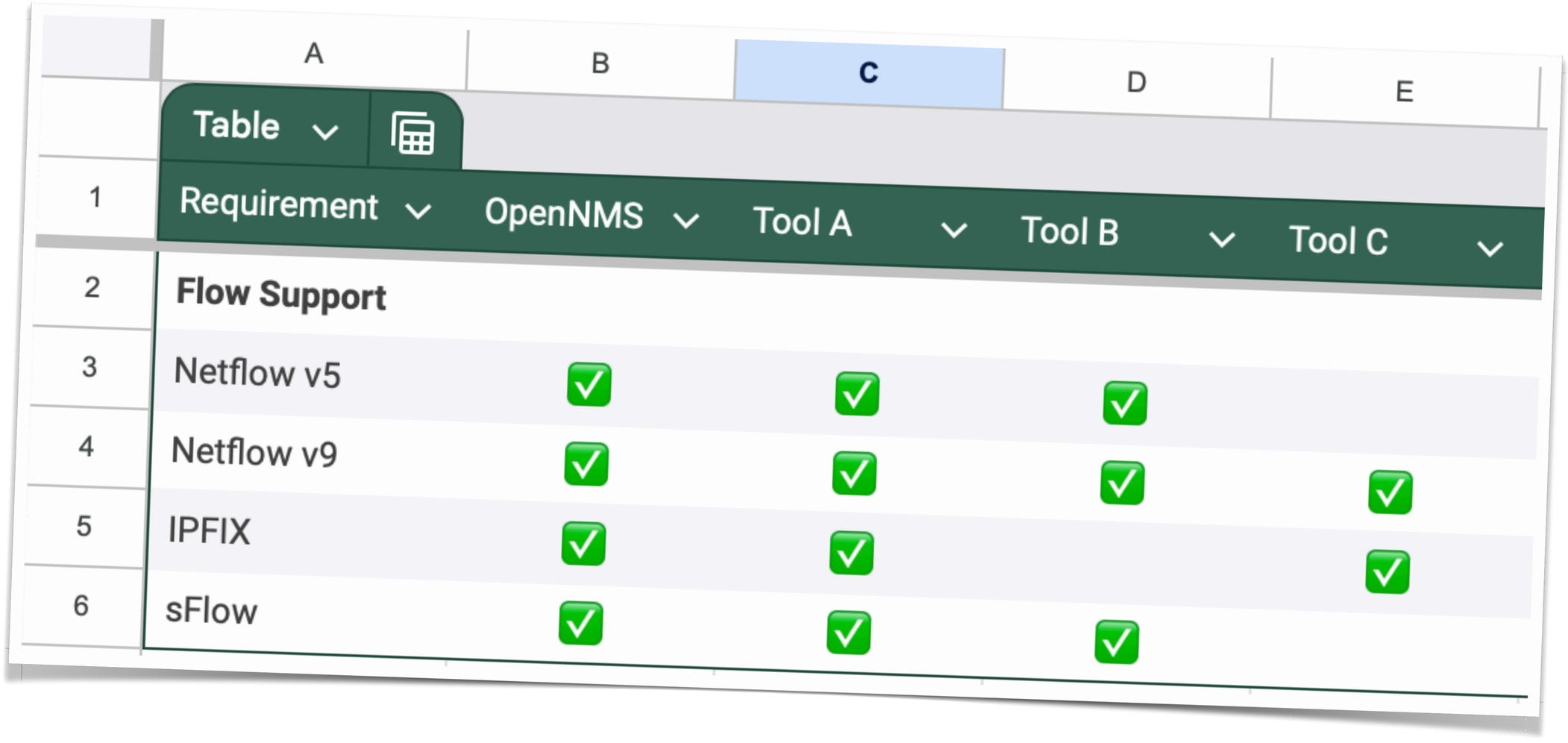


Name	Mean	Max	Min
mi de (In)	501 kb/s	6.31 Mb/s	0 b/s
mi de (Out)	-25.8 Mb/s	0 b/s	-317 Mb/s
ci e (In)	13.0 kb/s	1.14 Mb/s	0 b/s

Data Usage by Host (Top N)

Host	In	Out	ECN
ch.de	11.44 MB	311.44 MB	non-ect / no ce
da.de	7.01 MB	257.67 MB	non-ect / no ce
.de	5.17 MB	254.38 MB	non-ect / no ce
0	4.57 MB	202.06 MB	non-ect / no ce
52.230.152.243	1.12 MB	180.64 MB	non-ect / no ce
52.230.152.45	979.22 kB	174.89 MB	non-ect / no ce


elastic
Search Elastic
D
Discover
Options
New
Open
Share
Inspect
Save
netflow.application: https and node_exporter.foreign_id: mirror
KQL
Last 15 minutes
Show dates
Refresh
+ Add filter
netflow-*
Search field names
Filter by type 0
Available fields 55
Popular
netflow.ip_protocol_version
netflow.protocol
_id
_index
_score
_type
@clock_correction
@timestamp
@version
host
hosts
location
netflow.application
netflow.bytes
netflow.convo_key
netflow.delta_switched
netflow.direction
netflow.dscp
netflow.dst_addr
netflow.dst_addr_hostname
netflow.dst_locality
netflow.dst_port
netflow.ecn
netflow.first_switched
netflow.flow_locality
netflow.flow_records
netflow.flow_seq_num
14,245 hits
Chart options
1,200
1,000
800
600
400
200
0
15:02:00
15:03:00
15:04:00
15:05:00
15:06:00
15:07:00
15:08:00
15:09:00
15:10:00
15:11:00
15:12:00
15:13:00
15:14:00
15:15:00
15:16:00
Jun 20, 2024 @ 15:01:25.030 - Jun 20, 2024 @ 15:16:25.030
netflow.dst_port 443
netflow.ecn 0
netflow.first_switched Jun 20, 2024 @ 15:13:01.582
netflow.flow_locality public
netflow.flow_records 9
netflow.flow_seq_num 307,798
netflow.input_snmp 2
netflow.ip_protocol_version 4
netflow.last_switched Jun 20, 2024 @ 15:13:01.684
netflow.output_snmp 0
netflow.packets 27
netflow.protocol 6
netflow.sampling_algorithm Unassigned
netflow.src_addr 149.217.71.8
netflow.src_addr_hostname ftp.mpia-hd.mpg.de
netflow.src_locality public
netflow.src_port 56894
netflow.tcp_flags 30
netflow.tos 0
netflow.version Netflow v9
node_exporter.foreign_id mirror
node_exporter.foreign_source IONOS



	A	B	C	D	E
	Table				
1	Requirement	OpenNMS	Tool A	Tool B	Tool C
2	**Flow Support**				
3	Netflow v5	✅	✅	✅	
4	Netflow v9	✅	✅	✅	✅
5	IPFIX	✅	✅		✅
6	sFlow	✅	✅	✅	

Resources

- https://github.com/indigo423/OITC-2024
- https://docs.opennms.com/horizon/33/operation/deep-dive/flows/basic.html
- https://blog.sflow.com/2022/02/udp-vs-tcp-for-real-time-streaming.html
- https://opennms.discourse.group/t/how-to-use-pmacct-as-a-netflow-9-probe-on-ubuntu-linux-and-mac-os-big-sur/1160
- https://opennms.discourse.group/t/running-in-docker-and-receiving-flows-traps-or-syslog-messages-over-udp/1103
- https://www.varonis.com/blog/flow-monitoring
- https://chat.opennms.com/opennms/channels/opennms-discussion
- https://github.com/OpenNMS/elasticsearch-drift-plugin