

Mastering ntopng

Flow Aggregation and Traffic Rules

Nicolo' Maio
maio@ntop.org

Main Issues to Tackle

1. Monitor selected SNMP devices, hosts, network interfaces, host pools, and networks.
2. Easily gather statistics about the traffic generated by a specific application protocol or a couple of client-server pairs.























Presentation Outline

- SNMP Devices Rules
- Host/Net Interface/Host Pool/Network Rules
- Exercise of Network Interfaces Rules
- Aggregated Live Flows
- Examples of Aggregated Live Flows in ntopng

SNMP Devices Rules [1/7]

- **Simple Network Management Protocol (SNMP)** is an Internet Standard protocol for collecting and organizing information about managed devices on IP networks and for modifying that information to change device behaviour.

SNMP Devices Rules [2/7]

SNMP Devices Interfaces Rules    								
Show 10 entries		Device Filter +   Search: <input type="text"/>						
Device IP	SNMP Version	Chart	Device Name	Description	Interfaces With Errors	Time Since Last Poll	Last Poll Duration	Actions
192.168.2.1	v1		EdgeRouter-X-5-Port	office router	2	00:41	00:01	
192.168.2.83	v1		vsphere-idrac		1	00:41	00:02	
192.168.2.106	v1		MikroTik Ax3	RouterOS C53UiG+5HPaxD2H...		00:41	00:03	
192.168.2.120	v1		idrac-8YQXT72		1	00:41	00:02	
192.168.2.134	v2c		devele	Linux devele 6.2.0-26-ge...	1	00:41	00:01	
192.168.2.167	v2c		nTopSwitch	28-Port Gigabit Managed ...	1	00:41	00:08	
192.168.2.169	v1		ProCurve Switch 2510B-24	ProCurve J9019B Switch 2...	1	00:41	00:04	
192.168.2.175	v1		3Com Baseline Switch	3Com Baseline Switch 292...		00:41	00:04	

SNMP Devices Rules [3/7]

- Monitoring and discovering that a specific SNMP Device has exceeded traffic thresholds is not possible using the previously engaged alerts (such as Ingress Traffic, Egress Traffic, etc...)

SNMP Devices Rules [4/7]

- With the SNMP Devices Rules, it is possible to monitor a specific SNMP device or a specific interface of a specific SNMP device with interval frequency checks of 5 minutes, 1 hour or 1 day.

SNMP Devices Rules [5/7]

- The Threshold Rule can be an upper or lower bound of Bytes, Packets or Interface Errors.
- When a threshold is crossed ntopng will trigger an alert.

SNMP Devices Rules [6/7]

Select
the SNMP device

Select
the SNMP device port

Select
the metric

Select
the check frequency

Select
the rule threshold

Add Rule

Rule type **SNMP Device**

Device 3Com Baseline Switch (192.168.2.175) ▼

Interface GigabitEthernet1/0/10 (10) ▼

Metric Bytes (RX/TX) ▼

Check Frequency 5 Minutes ▼

Threshold Volume ▼ **KB MB GB** > < 1

NOTES

- Device: select the SNMP Device to be analyzed
- Interface: select the interface of the SNMP device that needs to be analyzed.
- Metric: select the metric to be analyzed (e.g. errors -> the SNMP metric errors)
- Frequency: select the frequency of the analysis (e.g. 5 Min -> analyzed every 5 minutes)
- Threshold: select the type of threshold (Volume, Throughput or Percentage), lowerbound or upperbound, and the threshold that, if exceeded, is going to trigger an alert
- Percentage Threshold: is calculated between the last two frequency checks (e.g. <1% with frequency 5 Min -> if the difference between precedent frequency and the last 5 minutes check is lower than 1% trigger and alert)

SNMP Devices Rules [7/7]

n

Shortcuts

Dashboard

Alerts

Flows

Hosts

Maps

Interface

Settings

Developer

Help

ens160

199.90 Kbps
213.30 Kbps

2

17

3

12

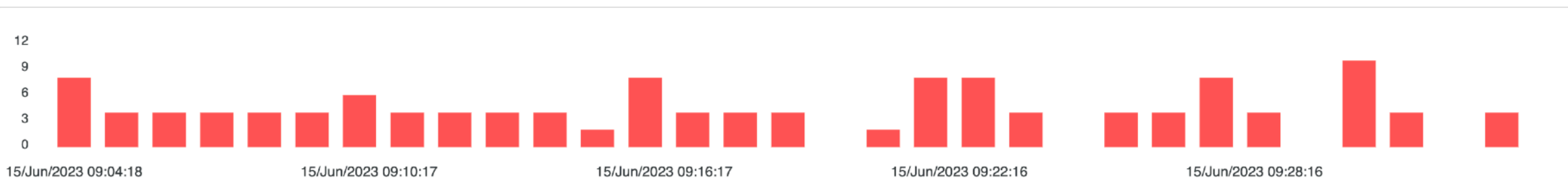
575

Search

Alerts Explorer | All 2 Host 2 Interface **SNMP** Flow MAC Address System User

Past Ack Engaged Last 30 Min 15/06/2023 09:04 → 15/06/2023 09:34 Apply

Severity >= Error x Filters



Show 10 Entries Search:

	Device IP	SNMP Interface	SNMP Device Name	Counts	Description
Id Crossed	192.168.2.237	X435-24P-4S Port 2	X435-24P-4S	1	Metric: Bytes (RX/TX) / Unit: Volume / Value: 0 Bytes / Threshold: < 1 GB
Id Crossed	192.168.2.237	X435-24P-4S Port 7	X435-24P-4S	1	Metric: Bytes (RX/TX) / Unit: Volume / Value: 0 Bytes / Threshold: < 1 GB
Id Crossed	192.168.2.237	X435-24P-4S Port 15	X435-24P-4S	1	Metric: Bytes (RX/TX) / Unit: Volume / Value: 0 Bytes / Threshold: < 1 GB
Id Crossed	192.168.2.237	X435-24P-4S Port 14	X435-24P-4S	1	Metric: Bytes (RX/TX) / Unit: Volume / Value: 0 Bytes / Threshold: < 1 GB
Id Crossed	192.168.2.237	X435-24P-4S Port 15	X435-24P-4S	1	Metric: Bytes (RX/TX) / Unit: Volume / Value: 0 Bytes / Threshold: < 1 GB
Id Crossed	192.168.2.237	X435-24P-4S Port 7	X435-24P-4S	1	Metric: Bytes (RX/TX) / Unit: Volume / Value: 0 Bytes / Threshold: < 1 GB

Host/Interface/HostPool/Network Rules [1/4]

- Same as SNMP Rules but for hosts, network interfaces, host pool and network.
- In this case is possible to active monitor a specific host, or a specific network interface or a specific host pool or a specific network with interval frequency checks of 5 minutes, 1 hour or 1 day.

Host/Interface/HostPool/Network Rules [2/4]

In case of Rule Type Host
indicate the Host,
Otherwise select an Interface or
Select an Host Pool or
Select a Local Network

Select the metric

Select
the check frequency

Select the rule threshold

Add Rule

Rule type

HostInterfaceHost PoolsNetworks

Target

A local host IP or '*' for checking all local hosts

Metric

Traffic

Check Frequency

5 Minutes

Threshold

Volume

KBMBGB

><

1

NOTES

- Target: insert the IP of a Local Host to be analyzed or a * (meaning that all Local Hosts has to be analyzed) or select a local network interface
- Metric: select the metric to be analyzed (e.g. DNS -> the DNS traffic)
- Frequency: select the frequency of the analysis (e.g. 5 Min -> analyzed every 5 minutes)
- Threshold: select the type of threshold (Volume, Throughput or Percentage), lowerbound or upperbound, and the threshold that, if exceeded, is going to trigger an alert
- Percentage Threshold: is calculcated beetwen the last two frequency checks (e.g. <1% with frequency 5 Min -> if the difference between precedent frequency and the last 5 minutes check is lower than 1% trigger and alert)

Add

Host/Interface/HostPool/Network Rules [3/4]

- **Metrics for the Host and Network Interface Rules:**

- Traffic RX / TX (or both),
- Score
- Application Traffic.

- **Metrics for the HostPools Rules:**

- Traffic RX / TX (or both),
- Active Devices,
- Active Hosts,
- Blocked Flows


- **Metrics for the Network Rules:**

- Broadcast Traffic RX / TX (or both)
- Traffic RX / TX (or both)
- Engaged Alerts
- Round Trip Time
- Score
- TCP Packets KeepAlive
- TCP Packets Lost
- TCP Packets Out-Of-Order
- TCP Retransmitted Packets

Host/Interface/HostPool/Network Rules [4/4]

In Actions menu
the edit and
delete rule
options are
present

en0



37.10 Kbps
57.30 Kbps

1

13

24

23 (1)

10

182

Search

3

Local Traffic Rules

Show

10

 entries

Target

Type

Metric

Check Frequency

Last Measurement

Threshold

Actions

PippoPool

Host Pool

Active Devices

5 Minutes

0

> 15

192.168.1.0/24

Network

TCP Packets Lost

5 Minutes

0

> 100

Showing 1 to 2 of 2 entries

«

<

1

>

»

NOTES

- Trigger an alert when a local host exceeds the specified traffic amount
- To add a new rule, click the '+' symbol on the right side above the table (next to the search)
- To remove a rule, click on the 'Actions' column button and then click onto 'Delete' on the row you want to remove

Exercise of Network Interfaces Rules

Exercise of Network Interfaces Rules [1/1]

- Set a Network Interface Rule with threshold > 1 KB
- Set a notification endpoint and recipient to receive a message on telegram when the Threshold is crossed.
- Restart ntopng
- (The alert name is 'Network Interface Volume Exceeded')

Aggregated Live Flows [1/11]

- To find the total traffic for a specific Application Protocol on the Live Flows page, a user needs to activate the protocol filter and sum the traffic bytes.

Aggregated Live Flows [2/11]

- With Aggregated Live Flows, it is easy to quickly discover the total traffic and various other information related to a specific Application Protocol.

Aggregated Live Flows [3/11]

- The current aggregation criteria are:
 - Application Protocol
 - Client
 - Server
 - Client-Server
 - Client-Server-Destination Port
 - Client-Server-App.Proto
 - Info

Aggregated Live Flows [4/11]

Clicking on the flows icon
Is possible to jump to the
live flows filtered by the
specific
row values of the
aggregation criteria

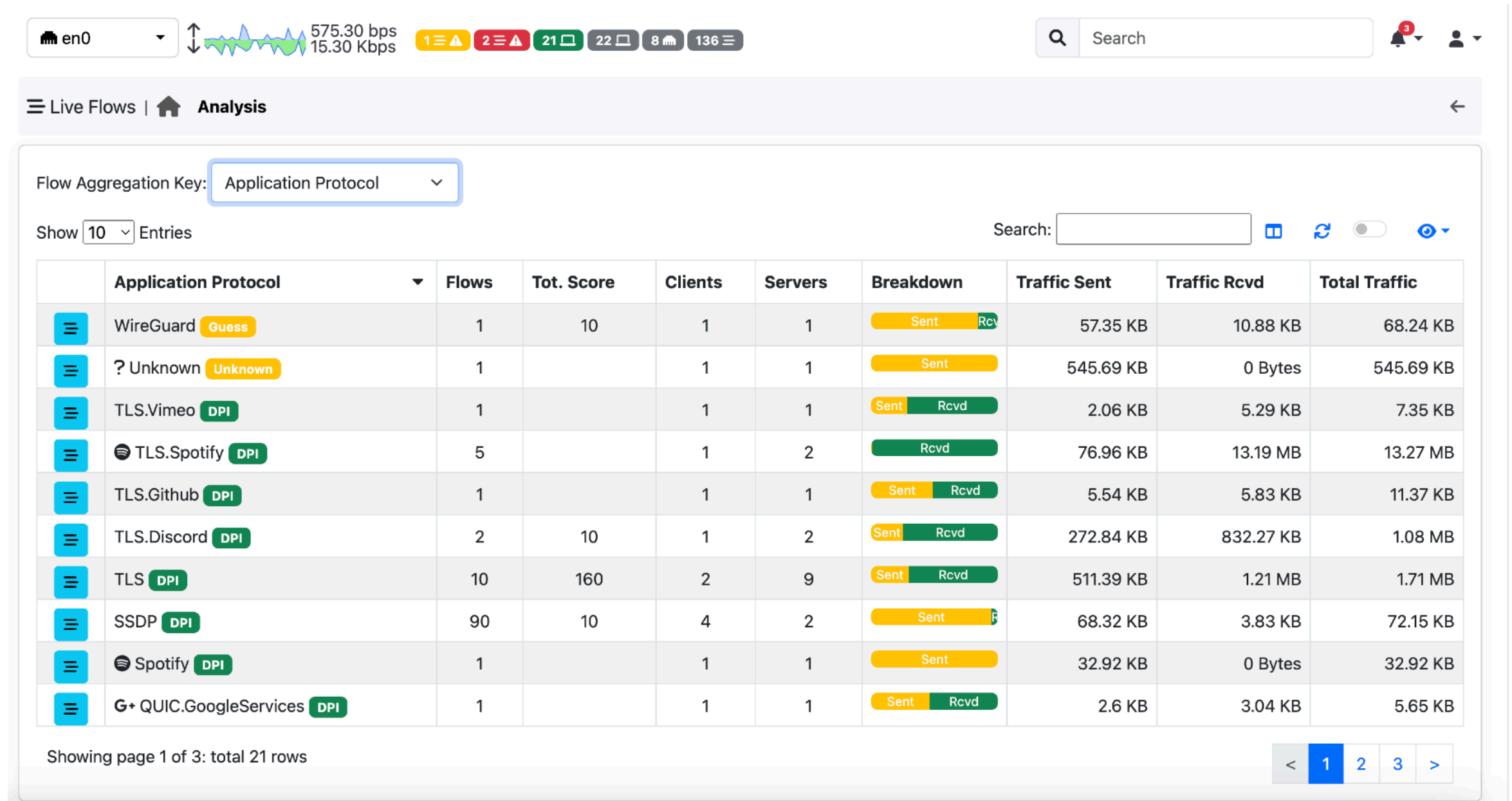
Clicking on the link
in the Client or Server Column
is possible to jump to the
Host details page

Client	Server	Flows	Tot. Score	Breakdown	Traffic Sent	Traffic Received
desktop-maio.homenet.telecomitalia.it	224.0.0.251	1		Sent	46 Bytes	
192.168.2.11	239.255.255.250	1		Sent	46 Bytes	
host-004.homenet.telecomitalia.it	224.0.0.251	1		Sent	79 Bytes	
mbp-di-nicolo.homenet.telecomitalia.it	224.0.0.251	1		Sent	87 Bytes	
fe80::101b:a729:c77d:e881	ff02::fb	1		Sent	99 Bytes	
macbook-pro-di-nicolo.local	ff02::fb	1		Sent	107 Bytes	
mbp-di-nicolo.homenet.telecomitalia.it	17.57.146.173	1	50	Sent Rcvd	166 Bytes	
mbp-di-nicolo.homenet.telecomitalia.it	h388x.homenet.telecomitalia.it	3		Sent	210 Bytes	
samsung.homenet.telecomitalia.it	224.0.0.251	1		Sent	248 Bytes	
mbp-di-nicolo.homenet.telecomitalia.it	h388x.homenet.telecomitalia.it	8	10	Sent Rcvd	690 Bytes	

Showing page 1 of 4: total 37 rows

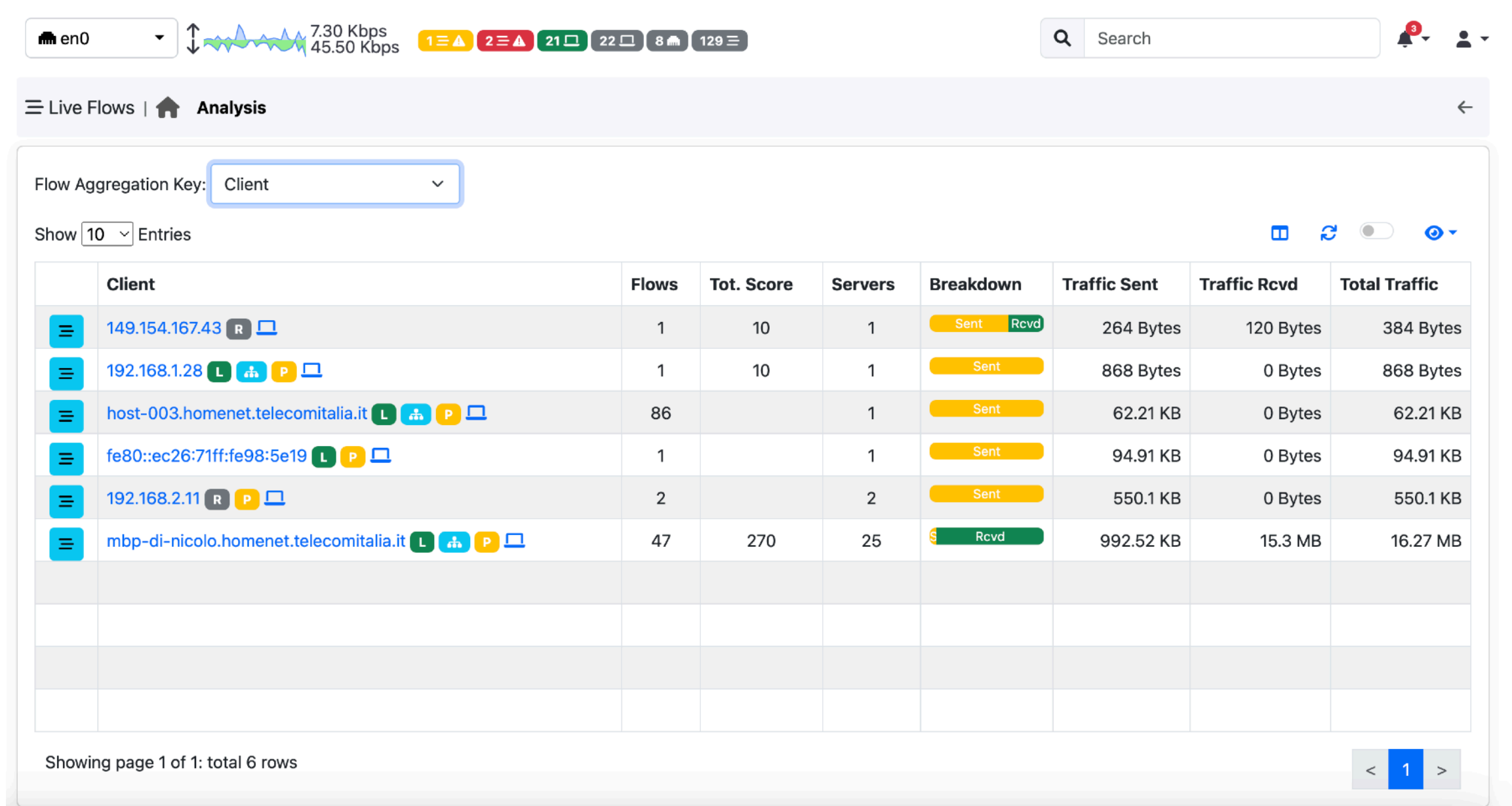
Aggregated Live Flows [5/11]

Application Protocol Criteria



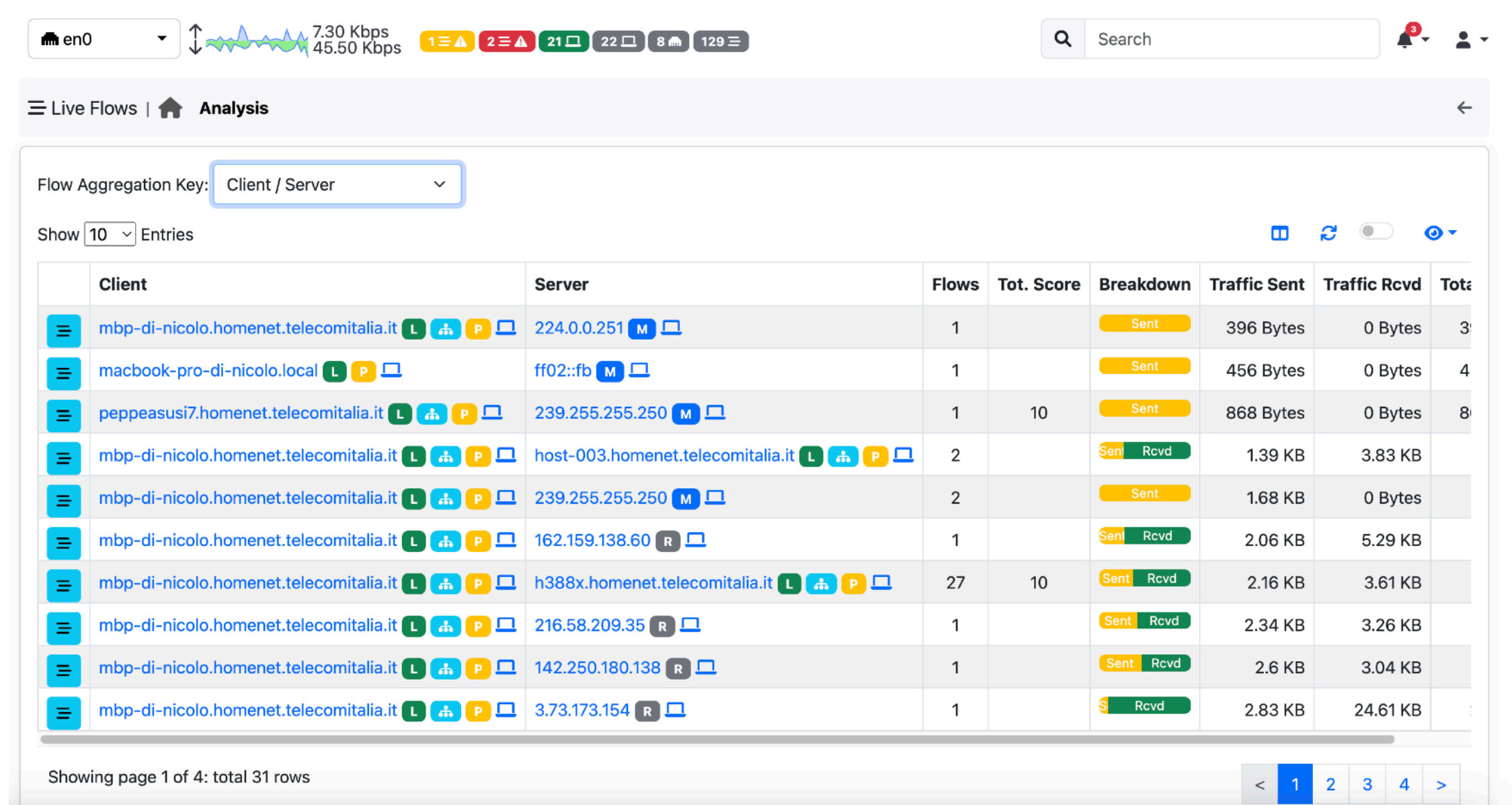
Aggregated Live Flows [6/11]

Client Criteria



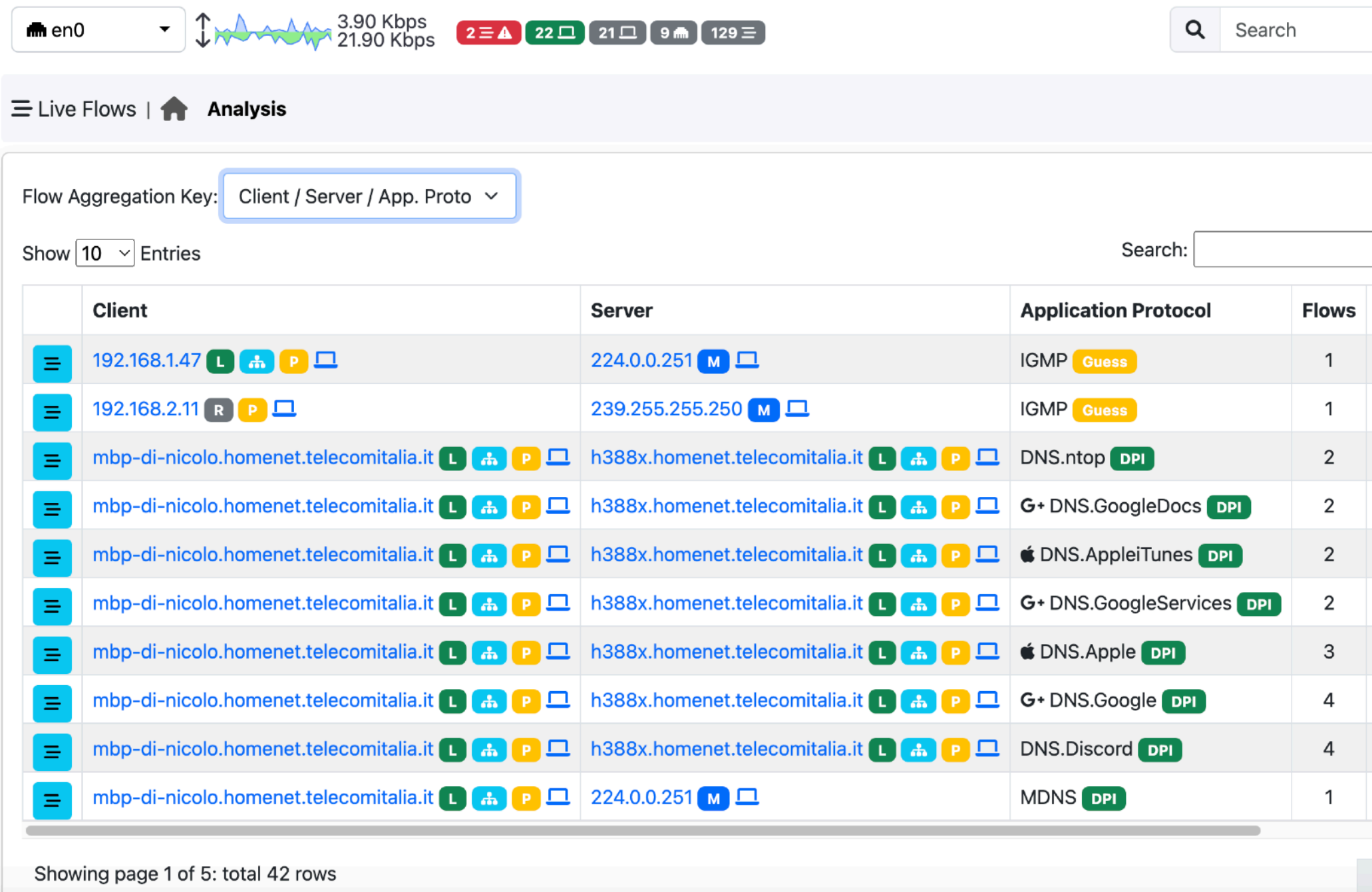
Aggregated Live Flows [7/11]

Client / Server Criteria



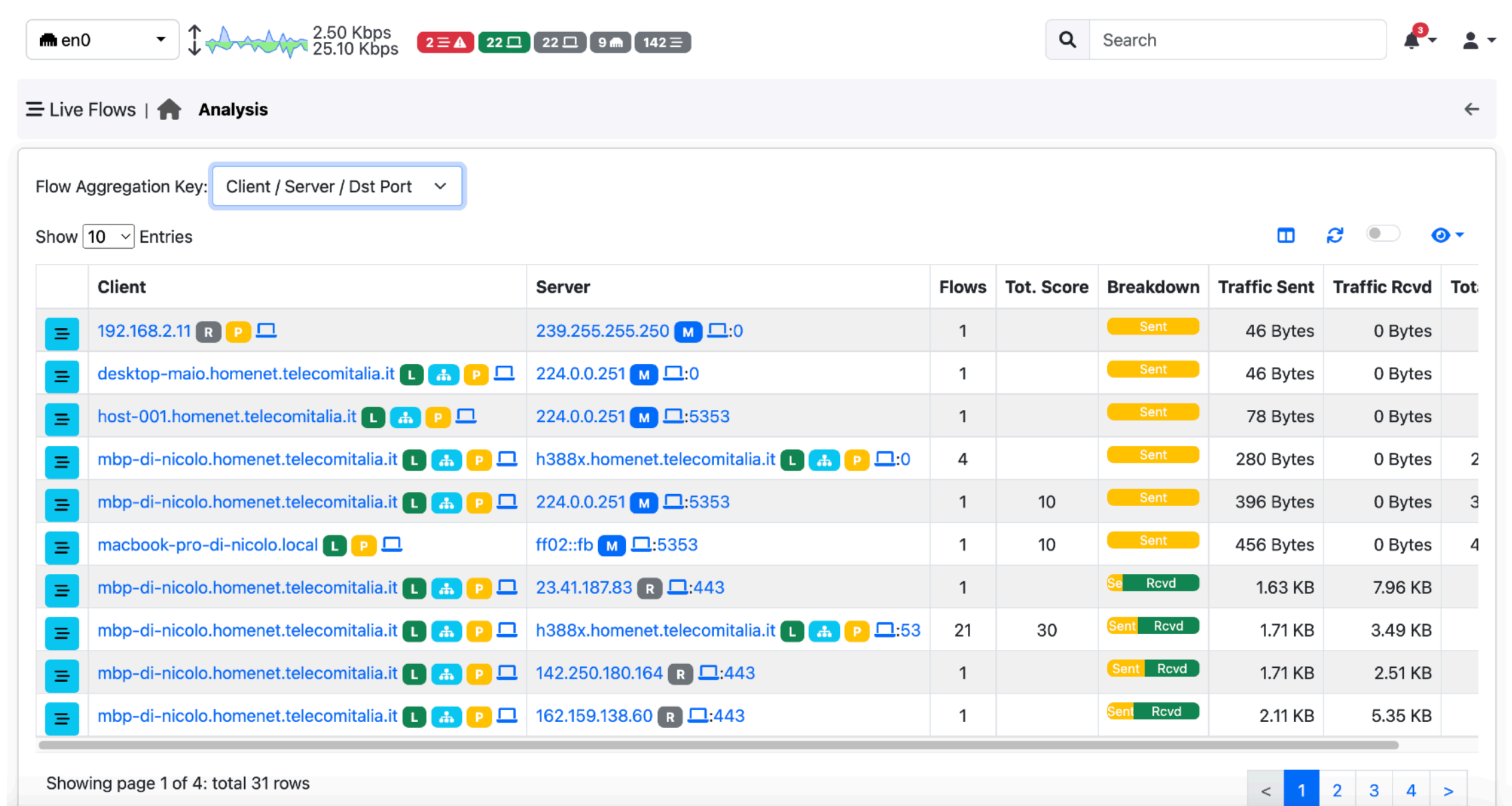
Aggregated Live Flows [8/11]

Client / Server / App. Proto



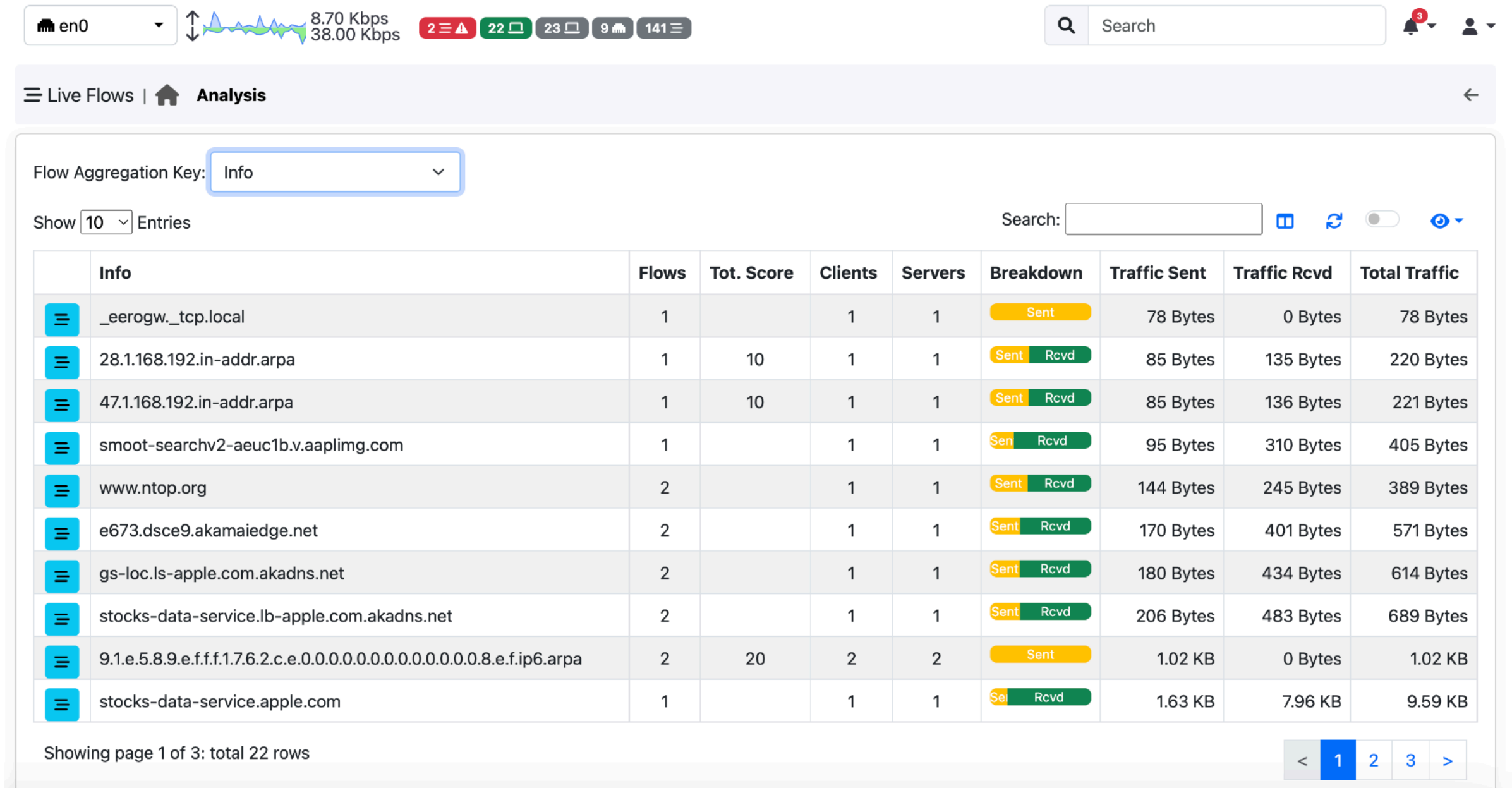
Aggregated Live Flows [9/11]

Client / Server / Dst. Port



Aggregated Live Flows [10/11]

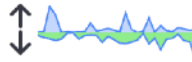
Info Criteria



Aggregated Live Flows [11/11]

Server Criteria

en0

1.70 Kbps
60.70 Kbps

2

22

23

9

142

Search

3

Live Flows

Analysis

Flow Aggregation Key:

Server

Show

10

 Entries

	Server	Flows	Tot. Score	Clients	Breakdown	Traffic Sent	Traffic Rcvd	Total Traffic
<div></div>	ff02::fb <div>M</div> <div></div>	1	10	1	<div>Sent</div>	563 Bytes	0 Bytes	563 Bytes
<div></div>	224.0.0.251 <div>M</div> <div></div>	3	10	3	<div>Sent</div>	607 Bytes	0 Bytes	607 Bytes
<div></div>	host-003.homenet.telecomitalia.it <div>L</div> <div></div> <div>P</div> <div></div>	1		1	<div>Sent</div>	714 Bytes	0 Bytes	714 Bytes
<div></div>	149.154.167.43 <div>R</div> <div></div>	1		1	<div>S</div> <div>Rcvd</div>	928 Bytes	12.93 KB	13.83 KB
<div></div>	17.57.172.11 <div>R</div> <div></div>	1		1	<div>Sent</div> <div>Rcvd</div>	1009 Bytes	3.13 KB	4.12 KB
<div></div>	23.41.187.83 <div>R</div> <div></div>	1		1	<div>Ser</div> <div>Rcvd</div>	1.63 KB	7.96 KB	9.59 KB
<div></div>	142.250.180.164 <div>R</div> <div></div>	1		1	<div>Sent</div> <div>Rcvd</div>	1.71 KB	2.51 KB	4.22 KB
<div></div>	17.36.206.5 <div>R</div> <div></div>	1		1	<div>Sent</div> <div>Rcvd</div>	1.81 KB	6.47 KB	8.28 KB
<div></div>	h388x.homenet.telecomitalia.it <div>L</div> <div></div> <div>P</div> <div></div>	25	30	1	<div>Sent</div> <div>Rcvd</div>	2 KB	3.73 KB	5.73 KB
<div></div>	17.57.172.10 <div>R</div> <div></div>	1		1	<div>Sent</div> <div>Rcvd</div>	2.04 KB	6.6 KB	8.63 KB

Showing page 1 of 3: total 30 rows

<

1

2

3

>

Examples of Aggregated Live Flows in ntopng



<https://github.com/ntop/ntopng>